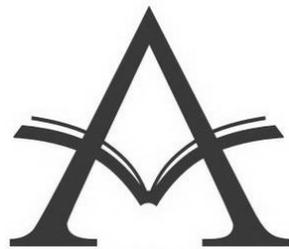


UNIVERSIDAD PERUANA DE LAS AMÉRICAS



ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

Los Delitos Informáticos y su influencia en la Integridad  
Personal, distrito de Chorrillos, Lima Metropolitana,  
2019.

PARA OPTAR EL GRADO DE BACHILLER EN DERECHO

AUTOR:

Carlos Alberto Reyes Valdivia

ASESOR:

Mg. Andrés José Boric Santos

LÍNEA DE INVESTIGACIÓN:

Delitos Informáticos

LIMA, PERÚ

JUNIO, 2020

## **DEDICATORIA**

Dedico este trabajo a mi familia a mi hermosa madre Ana VALDIVIA MORALES, a la cual tengo mucho, pero mucho amor, un sentimiento infinito y a mi fiel hermano que es un apoyo incondicional en mis convicciones.

## **AGRADECIMIENTO**

Un autor siempre tiene que ser agradecido con aquellas personas, colaboraron en su desarrollo, en especial a mis catedráticos que se convirtieron en nuestros amigos, con sus consejos nos supieron guiar, dar un impulso permanente, a mis compañeros y promociones de EO-PNP, de los cuales solo acabamos cinco y al ángel que nos cuida, Katty COLONIA BALDEON, que tuvo una partida muy prematura al cielo, que sin su responsabilidad no estaría desarrollando esta investigación.

## RESUMEN

La presente investigación estuvo basada en “Los Delitos Informáticos y su influencia en la integridad personal, distrito de Chorrillos, Lima Metropolitana, 2019”. El trabajo consistió en conocer y determinar de qué manera los delitos informáticos influyen en la integridad de las personas. La población estuvo determinada por los residentes Personas de 18 a 30 años, del distrito de Chorrillos, y la muestra estuvo conformada por un grupo no probabilístico por conveniencia.

El instrumento de medición utilizado fue el cuestionario, cuya técnica se basó en la técnica. La metodología de investigación fue no experimental, de enfoque cuantitativo, de corte transversal, de diseño no experimental. Con relación a los resultados, se evidenció la relación positiva y significativa entre ambas variables de estudio, es decir, a medida que los delitos informáticos se incrementan también se verá perjudicada la integridad personal. Cabe señalar que, este estudio permite analizar, plantear recomendaciones para combatir de mejor manera los delitos informáticos, asimismo proteger la integridad de las personas. Finalmente, se concluye que, los delitos informáticos son hechos ilícitos que están en un desarrollo muy nocivo para la seguridad, lo que nos conlleva atener nuevas armas jurídicas para poder abordar correctamente estos hechos.

### **Palabras Claves**

Palabras Clave: Delito informático, integridad personal, Ley N° 30096, ONGEI.

## ABSTRACT

This investigation was based on "Computer Crime and its influence on personal integrity, Chorrillos district, Metropolitan Lima, 2019". The work consisted of knowing and determining how computer crimes influence the integrity of people. The population was determined by the residents of 18 to 30 years old, from the Chorrillos district, and the sample was made up of a non-probabilistic group for convenience. The measuring instrument used was the questionnaire, whose technique was based on the technique. The research methodology was non-experimental, quantitative approach, cross-sectional, non-experimental design. Regarding the results, the positive and significant relationship between the two study variables was evident, that is, as computer crimes increase, personal integrity will also be impaired. It should be noted that this study allows analyzing, making recommendations to better combat computer crimes, as well as protecting the integrity of people. Finally, it is concluded that computer crimes are illicit acts that are in a very harmful development for security, which leads us to have new legal weapons to be able to properly address these facts.

### Keywords

Computer crime, personal integrity, Law No. 30096, ONGE

## TABLA DE CONTENIDO

DEDICATORIA .....	ii
AGRADECIMIENTO .....	iii
RESUMEN.....	iv
PROBLEMA DE LA INVESTIGACIÓN .....	8
<b>Descripción de la realidad problemática</b> .....	8
<b>Formulación del problema general</b> .....	10
<b>Problema general</b> .....	10
<b>Problemas específicos</b> .....	10
<b>Objetivos de la investigación</b> .....	11
<b>Objetivo General</b> .....	11
<b>Objetivos Específicos</b> .....	11
<b>Justificación e importancia de la investigación</b> .....	12
<b>Justificación teórica</b> .....	12
<b>Justificación practica</b> .....	12
<b>Justificación social</b> .....	12
MARCO TEÓRICO .....	14
<b>Antecedentes</b> .....	14
<b>Internacionales</b> .....	14
<b>Nacionales</b> .....	19
<b>Bases teóricas</b> .....	22
<b>Delitos informáticos</b> .....	22
<b>Bien jurídico tutelado</b> .....	23
<b>Integridad personal</b> .....	24
<b>Definición de términos básicos</b> .....	26
CRONOGRAMA DE ACTIVIDADES .....	30
RECURSOS Y PRESUPUESTO .....	32

REFERENCIAS .....	33
APORTE CIENTÍFICO O ACADÉMICO .....	38
ANEXOS.....	40

## PROBLEMA DE LA INVESTIGACIÓN

### Descripción de la realidad problemática

El delito informático es considerado como aquella acción típica, antijurídica y culpable efectuada por medios informáticos o cuya acción busca modificar los datos de un dispositivo electrónico, concepto que trata de englobar la perspectiva informática, implicando el concepto generalizado de delito e incluyendo la utilización del medio informático, esto presupone afectar la integridad personal en sus niveles psicológicos, moral y físico tanto en adultos como en adolescentes y niños, quienes son aún más vulnerables ante este tipo de delitos que, ocurren en un contexto totalmente expuesto a cambios tecnológicos e informáticos.

En el contexto internacional, de acuerdo con Perfil (2020) señala que el ciberespacio es fuente de amenazas a la seguridad, y el desafío de Naciones Unidas. Cabe señalar que la ONU ha concluido las negociaciones de cara a una futura Convención sobre Delitos Informáticos, la cual buscará remediar una notoria falencia en estos temas, donde la sociedad internacional en su conjunto no ha logrado articular consensos ni esbozar estrategias multilaterales. Tomar en consideración que, los últimos esfuerzos en este campo corresponde al Consejo de Europa con su Convenio sobre la Ciberdelincuencia (o Convenio de Budapest), en rigor de verdad una norma regional.

En el entorno nacional, de acuerdo con Andina (2020) los delitos informáticos más frecuentes en el Perú registrados por la División de Investigación de Delitos de Alta Tecnología (Divindat) de la policía, la cual registró 3,012 denuncias de fraudes electrónicos, pornografía infantil, suplantación de identidad y otros delitos informáticos durante el periodo 2019. Asimismo, cabe mencionar que la mayor cantidad de denuncias se enfocan en el delito contra el patrimonio. Los fraudes informáticos y sus subtipos alcanzaron 2,097 denuncias durante el 2019, esto es, la cifra se elevó en más de 8% en relación al 2018, que cerró con 1,928 casos. La suplantación de identidad es otra amenaza digital recurrente en el país con 247 casos en el 2019. Por otra parte, los delitos informáticos relacionados a casos de pornografía infantil han sumado 237 casos en el mismo periodo, lo que

evidencia la problemática nacional y como tal, el trabajo a cargo de la policía y a nivel gubernamental por identificar y tomar acciones inmediatas para terminar con esta impunidad. Aunque Perú cuenta también con una Ley N° 30096 de Delitos Informáticos, aún quedan muchos aspectos por mejorar o perfeccionar a nivel de ley y reglamento, es por ello que el desarrollo de investigaciones respecto a este materia de análisis.

En relación a esta problemática actual o coyuntura expuesta, donde los delitos informáticos a cargo de personas naturales por motivos de diversa índole o por personas jurídicas sea por espionaje, distorsión de información, entre otros. La presente investigación pretende desarrollar la formulación del problema delimitándose a un ámbito particular y zona geográfica determinada, donde se ve afectada la integridad personal, es decir, la vulneración del derecho de la persona humana, a través de la siguiente interrogante: ¿De qué manera los delitos informáticos influyen en la Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019?

## **Formulación del problema general**

### **Problema general**

¿De qué manera Los Delitos Informáticos influyen en la Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019?

### **Problemas específicos**

¿De qué manera Los Delitos Informáticos Contra la indemnidad y libertad sexual influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019?

¿De qué manera Los Delitos Informáticos Contra la intimidad y el secreto de las comunicaciones influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019?

¿De qué manera Los Delitos Informáticos Contra datos y sistemas informáticos influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019?

¿De qué manera Los Delitos Informáticos Contra el patrimonio influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019?

¿De qué manera Los Delitos Informáticos Contra la fe pública influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019?

## **Objetivos de la investigación**

### **Objetivo General**

Determinar de qué manera Los Delitos Informáticos influyen en la Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019.

### **Objetivos Específicos**

Determinar de qué manera Los Delitos Informáticos Contra la indemnidad y libertad sexual influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019.

Determinar de qué manera Los Delitos Informáticos Contra la intimidad y el secreto de las comunicaciones influyen en la Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019.

Determinar de qué manera Los Delitos Informáticos Contra datos y sistemas informáticos influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019.

Determinar de qué manera Los Delitos Informáticos Contra el patrimonio influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019.

Determinar de qué manera Los Delitos Informáticos Contra la fe publica influyen en la Integridad Personal distrito de Chorrillos, Lima Metropolitana, 2019.

## **Justificación e importancia de la investigación**

### **Justificación teórica**

El valor teórico se sustenta en que los resultados de la investigación podrían generalizarse e incorporarse al conocimiento científico y además servirán para llenar vacíos cognoscitivos existentes o refutar resultados de otras investigaciones o ampliar un modelo teórico (Silvestre y Huamán, 2019, p 172). En la presente investigación, se utilizan las teorías relacionadas a las variables delito informático e integridad personal, de donde se exponen los elementos, principios y aspectos vinculados para contrastar su validez actual y con otras investigaciones.

### **Justificación práctica**

La importancia práctica se manifiesta en el interés del investigador por acrecentar sus conocimientos, obtener el título académico o, si es el caso, por contribuir a la solución de problemas concretos que afectan a organizaciones empresariales, públicas o privadas. (Valderrama, 2019 p 141). A este respecto, se busca analizar de qué manera los delitos informáticos influyen en la integridad personal para así presentar propuestas que coadyuven a combatir los excesos posibles en este ámbito del derecho.

### **Justificación social**

La relevancia social de esta investigación se da cuando el trabajo presentado va a resolver problemas sociales que afectan a un grupo social, como el empoderamiento de las mujeres campesinas o la aplicación del método psicosocial en la alfabetización de iletrados del medio rural. (Ñaupas, Valdivia, Palacios y Romero, p 221). En este caso, se busca beneficiar al ciudadano en general, quien utiliza con suma recurrencia tecnologías de información y comunicación.

**Justificación académica**

La importancia académica de la presente investigación está dada porque ésta representa un aporte para la comunidad universitaria y para los investigadores en derecho relacionados a temas de delitos informáticos e integral personal y pública interesado en la materia, y así contribuir con mayor información al respecto en las variables de estudio, con ello revalidar aspectos sumamente importantes como los derechos individuales del ser humano frente a los cambios tecnológicos de la actualidad.

## MARCO TEÓRICO

### Antecedentes

#### Internacionales

En el artículo científico desarrollado por Velastegui (2019) titulada “ Los Delitos Informáticos y su incidencia en la provincia de Pastaza”, esta revista científica tuvo como objetivo un análisis crítico y reflexivo, donde las maniobras digitales son adosados a hechos ilícitos en la provincia de Pastaza, el como la tecnología es más amigable con la población, pero también la pone en riesgo a que sufran más hechos ilícitos por medio del uso de esta tecnología, que se vuelve parte de uno por cada día que avanza. La metodología realizada tiene un enfoque cuali-cuantitativa, tuvo como población a la provincia de Pastaza en el país de Ecuador, la muestra fue representativa, para conocer su opinión y valoración. Se utilizó la recolección de datos mediante entrevistas y encuestas que permitieron al investigador recoger información muy relevante sobre el problema ya investigado.

Teniendo unos resultados muy alarmantes, siendo la Provincia de Pastaza que no cuenta con ningún tipo de oficina que se encarga de manejar la estadística de los reportes de en la actualidad y teniendo una crecida inminente de uso de maniobras digitales, y la minimización de analfabetismo digital, logrando formar estrategias que logren disminuir el alto índice de estos delitos que aqueja y aquejara a la población de Pastaza, se concluyó que los delitos informáticos, se presentan con mayor continuidad en la difamación y calumnias, son muy comunes en las redes sociales teniendo un daño directo al honor y a la honra de personas naturales y jurídicas, la afectación de estos delitos al orden económico es incalculable, por motivo que estos hechos se dan con el desconocimiento de las personas, teniendo que implementar mejores controles y políticas de seguridad.

En la investigación desarrollada por Ruiz (2016) titulada “Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos” para la obtención de título de abogada. Tuvo como objetivo, dar a conocer una visión clara de los delitos informáticos, poniendo énfasis sobre los delitos que transgreden los derechos constitucionales, que se generan por el uso incorrecto de esta por personas que tienen una capacidad alta de desarrollo en maniobras digitales, buscando encontrar alternativas a estos hechos que se presentan en acciones como lo son el uso de correo electrónico, redes sociales, el uso de pagos por internet, el uso de tarjetas. Su metodología que utilizó el investigador con un enfoque cualitativo y cuantitativo, no experimental, transversal, con una población de 30 personas, con la utilización de técnicas de entrevista, encuesta y análisis documental, esta investigación nos da como resultados, en lo actual los medios de comunicación se realizan de una forma inmediata o mejor dicho la celeridad del intercambio de información, lo que ha hecho que haya un desarrollo muy masivo de la tecnología, teniendo una conclusión, los delitos informáticos no solo afectan el patrimonio de muchas personas, también afectan la privacidad de una persona o de un colectivo, la falta de conocimiento de la tecnologías de información y la comunicación por parte de los operadores de justicia, es por el motivo que se omiten ciertos procedimientos para determinar la responsabilidad de los autores de estos hechos ilícitos.

En la investigación desarrollada por Maldonado (2016) titulada “Los delitos informáticos y el derecho constitucional a la seguridad jurídica” para la obtención del título de abogado de los tribunales de la República. Tuvo como objetivo general realizar un estudio de cómo los delitos informáticos inciden en el derecho constitucional a la seguridad ciudadana según los casos presentados en la ciudad de Babahoyo. Para ello, la metodología siguió un proceso de paradigma crítico y propositivo, de enfoque cuali-cuantitativo, asimismo de nivel descriptiva de tipo aplicada, con método deductivo e inductivo. La población estuvo conformada por 55 funcionarios de la Unidad Judicial Penal de la ciudad de Babahoyo, y la muestra fue de tipo censal. La técnica utilizada fue la encuesta para lograr recolectar datos de los

encuestados, esto mediante el instrumento de medición denominado cuestionario.

Los resultados permitieron determinar que son las personas las principales víctimas de este tipo de delitos, por tanto, deben tomar conciencia de la relevancia de aplicar métodos de seguridad informática en sus sistemas domésticos o empresariales a modo de combatir y evitar al máximo sufrir los efectos de estas acciones ilícitas. Finalmente, se concluye que los delitos informáticos representan hoy en día un acto ilícito que afecta en mayor medida a aquellas personas que no poseen suficiente preparación o conocimientos informáticos, siendo vulnerables sino logran capacitarse oportunamente. Asimismo, se demanda la regulación efectiva a través de un marco normativo que contemple la protección de datos e integridad personal en razón del ejercicio y goce de sus derechos respaldados por la Constitución.

Esta investigación esta desarrolla por Echevarría (2015) que tiene como título “Los Delitos Informáticos y El Derecho Constitucional a la Seguridad Publica”, para la obtención del título como abogada de los Juzgados y Tribunales de la República del Ecuador, tiene como objetivo general, tener que analizar como los delitos actuales, como lo son los delitos informáticos, inciden en el derecho constitucional ya que la tecnología se ha vuelto un factor muy amigable para el uso de todas las personas, enfocados en los delitos con la seguridad pública según los casos presentados en la Fiscalía General del Estado en el periodo 2014, la metodología cualitativa y cuantitativa, teniendo una población de 152 personas entre en fiscales, agentes investigadores, abogados en libre ejercicio, personas afectadas, con una muestra de 109 lo cual ayuda para el análisis respectivo. Tuvo como técnica a la encuesta, con la utilización de los instrumentos con un cuestionario de encuesta dirigido Fiscales, Agentes Investigadores, y personas afectadas.

Esta investigación tiene como resultado de ella que el país de Ecuador está en constante cambios sobre las investigaciones de los delitos informáticos, sin embargo, se tiene que mejorar el mecanismo que nos permite que todas las investigaciones frente a estos delitos tengan una dirección adecuada, dentro de un marco legal adecuado para realizar una eficiente acción frente a ello.

En esta revista digital por Narváez y Recalde (2018) con título “El Delito Informático en América”, nos presenta un objetivo que la legislación penal americana tiene que adecuarse a los delitos que se presentan en la actualidad como lo son los delitos informáticos, con una metodología cuantitativa y cualitativa, corte transversal, no experimental. Con una población y una muestra la cual es en general y no se precisa la cantidad, con técnica de entrevistas y encuestas y su instrumento un análisis documental.

Los resultados de esta investigación, es que estos delitos informáticos afectan directamente a la intimidad y el honor de una persona, así mismo el uso de identidad de manera ilícita y muchas variedades de delitos que se van innovando día a día. Concluyendo que todo este tipo de variedad de delitos es un fenómeno social que afecta a miles de personas en todo el mundo, teniéndose que tipificar estas conductas como figuras penales, para poder controlar y minimizar este tipo de hecho delictivos.

En la investigación desarrollada por Maldonado (2014), “El Delito Informático, vulnera el principio de la garantía constitucional y legal, sobre el honor de las personas establecidos en la constitución de La República”. Esta investigación tuvo como objetivo profundizar el estudio del Delitos Informático, su afectación a los principios constitucionales, quela carta magna de cada país defiende, teniendo como raíz principal la protección sexual, física y psicológica a consecuencias de maniobras digitales, teniendo múltiples hechos ilícitos llamados Delitos Informáticos. Teniendo una metodología, con un enfoque cuantitativa, no experimental, transversal con método inductivo y deductivo. La población 30 abogados, utiliza las técnicas de lectura científica, la cual ayudo al investigador a recolectar de una gran cantidad de información especializada, las encuestas lo realizan a abogados de libre ejercicio y a cinco jueces, donde se obtiene una gran cantidad de datos, para falsear la hipótesis de la investigación. Instrumentos encuesta y análisis documental.

Tiene como resultado esta investigación que no encuentra tipificación y penalización al delito informático y en sus variedades, teniendo en cuenta que el estado tiene que brindar protección necesaria a todas las naciones por medio la ley.

Se concluye que esta investigación si afecta de manera nociva las garantías constitucionales de la persona como lo son la integridad, física, moral

y sexual, para esta investigación no encuentra una tipificación exacta que establezca un abordaje de la acción ilícita, para esta conducta.

Esta investigación de Posso(2014), con el título “Los Delitos Informáticos y la violación de los derechos constitucionales del ofendido”, la cual tiene como objetivo tocar a fondo la realidad de los Delitos Informáticos en el Cantón Ambato, la regulación que tiene esta ciudad frente a estos delitos y su preparación para la formación de todo el talento humano, que va a realizar la investigación de estos delitos, así como identificar todo tipo de delitos conexos y el tratamiento de los mismos. Tiene una metodología cuantitativa y cualitativa, tiene como población a 100 personas, entre jueces, fiscales, abogados de libre ejercicio y víctimas de delitos informáticos, con una muestra de 32 personas de la ciudad de Ambato, utilizando técnicas encuestas y observación, esta investigación tiene como resultado, que esta investigación demuestre la realidad actual y busca implantar una adecuada aplicación de justicia teniendo como herramienta el código penal vigente de este país. Se concluye que en la actualidad los delitos así como todo, se va desarrollando, teniendo en cuenta que los hecho ilícitos siempre buscan la forman de querer superar a fuerzas del orden, para poder obtener un beneficio de dinero lo cual afecta a la personas que hacen el uso de la tecnología y son sorprendidos por maniobras digitales, se encuentran vacíos legales tanto a nivel nacional como internación, teniendo un impacto los delitos informáticos donde cada vez se requiere el personal capacitado para hacer una lucha frontal frente a esto.

## Nacionales

Esta investigación de Chilcon (2019), la cual tiene como título “El Ciberdelito en el Perú y su incidencia en la seguridad nacional”, que tiene como objetivo establecer el cómo afecta estos delitos que afectan a los ciudadanos que hacen uso de la tecnología y que como puede afectar a la seguridad nacional de Perú, tiene una metodología con un enfoque cuantitativo con un alcance descriptivo explicativo y un diseño de investigación no experimental, la población de esta investigación se constituye principalmente en directores y personal con capacidad de uso de un adecuado manejo de la tecnología como lo son la Policía Nacional del Perú, Ministerio Público y Poder Judicial, teniendo una población de 580 funcionarios, una muestra de 231 personas, utilizando una técnica cuestionario tipo Likert, y el uso de la prueba Chi Cuadrado para la demostración de las Hipótesis, como resultado de esta investigación que el ciberdelito alcanzado en el Perú un nivel elevado en víctimas por el uso de tecnología que por ola de aplicaciones y de redes sociales, hace que cada día aumente la población posible víctima de estos hechos ilícitos.

Teniendo la conclusión que el ciberdelito es un delito que se encuentra en crecida que no se está adoptando medidas de control y con el avance de la tecnología y el desarrollo de las capacidades de las personas que hacen, que estos hechos ilícitos afecten a la seguridad nacional, para cual esta investigación se recomienda implementar estrategias a largo plazo para el correcto abordaje de estos nuevos delitos.

Esta investigación de Chávez (2017), con el título “El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de Lima Norte, 2017”, que tiene como objetivo establecer que tanto afecta los delitos informáticos, específicamente los delitos contra datos y sistemas informáticos, los cuales afectan directamente los derechos fundamentales a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017. La metodología tiene un enfoque cuantitativo, alcance explicativo, diseño no experimental, transversal, correlacional – causal, con una población de 510 abogados y una muestra de 220 personas, la técnica utilizada fue la encuesta y como instrumento un cuestionario por cada variable, se tiene como resultado de esta investigación,

se llega a comprobar que el delito contra datos y sistemas de información influye contra el derecho fundamental a la intimidad personal, en conclusión se debe capacitar al personal que a todos los operadores que hacen lucha frontal a estos delitos para que de esta forma no se vulneren todo tipo de medio de prueba que puede servir como material idóneo, para contrarrestar este tipo de delitos.

En esta investigación de Zorrilla (2018), tiene como título “Inconsistencias y ambigüedades en la ley de delitos informáticos ley N° 30096 y su modificatoria ley N° 30171, que imposibilitan su eficaz cumplimiento”, tuvo como objetivo general determinar de qué manera se muestran las inconsistencias de la ley y que imposibilita su eficaz cumplimiento, con un metodología cuantitativa y cualitativa, transversal, con la encuesta como técnica, cuestionario como instrumento y una muestra de 30 profesionales de derecho.

Tuvo como resultado de la investigación, que la población donde se realiza la investigación manifiesta que si hay inconsistencias normativas para abordar este delito y que fue muy necesario que la ley de delitos informáticos tuviera su modificatoria. Concluyendo que hay varios artículos que presentan imprecisión en su redacción originando confusión en sus operadores, en el Perú no hay ley que defina correctamente los delitos que se presentan con mayor frecuencia en las redes sociales.

Esta investigación de Sequeiros (2016), tiene como título “Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano-2015”, teniendo una metodología descriptiva, cuantitativa, no experimental, transversal, con encuesta como técnica y cuestionario como instrumento, con una muestra de 30 persona con la profesión de fiscales, el resultado de esta investigación nos presenta la realidad del ministerio público, donde sus miembros de la provincia de Huara, nos da indicio de lo compleja de la situación, de la preparación y la información que ellos manejan para aplicar correctamente las leyes, frente a un hecho a un delito informático, que todos los días va innovando y así mismo se tiene que realizar modificaciones en las leyes.

Se concluye que los delitos informáticos, no debe limitar a la población de hacer uso de la tecnología ya que es un medio del cual no simplifica procesos, en donde se necesita más presencia del está para así dar el soporte de seguridad que corresponda para así poder llegar un gobierno digital cabal. Donde los ciudadanos puedan hacer sus funciones, desde el punto donde se encuentren y poder lograr la integridad de información, en la organización.

## **Bases teóricas**

Desde un enfoque del bien jurídico Chávez (2018) en base a lo propuesto por Franz Von Liszt, este bien es el “interés vital” que protege la sociedad, el cual no necesariamente es reconocido de manera constitucional, a su vez Kierszenbaum (2009) opina al respecto:

- Un bien jurídico es de interés vital porque este pasa a ser reconocido por una norma jurídica cumpliendo las características de ser importantes para el desenvolvimiento y desarrollo de una sociedad.
- El interés es parte de la convivencia humana, lo cual la dinamiza
- Para que un interés sea reconocido jurídicamente este se encuentra sujeto al Derecho Internacional y el Derecho Constitucional, el cual ordenara el Derecho Penal.

Por tal motivo se puede mencionar que el derecho es un medio para la garantía de satisfacer necesidades sociales lo cual se impone a las personas para la prevención de actos ilícitos.

Es necesario realizar un acercamiento conceptual desde una mirada del derecho a lo que se concibe como delito informático e integridad personal

## **Delitos informáticos**

De acuerdo con Villavicencio (2014) los delitos informáticos se encuentran relacionados con el concepto de comisión del crimen mediante el empleo de medios tecnológicos e internet. Son aquellas acciones que burlan los sistemas de seguridad, sistemas de datos o correos haciendo uso de una clave de acceso, donde las TICs (Tecnologías de la información y comunicación)son el medio para la ejecución de dichas conductas.

Se puede clasificar en tres tipos de delitos informáticos: manipulación informática, sabotaje informático y acceso no autorizado a datos, estos son los modos del delito informático mas no las categorías.

Por otro lado, la INTERPOL (2013) categoriza los delitos informáticos en diferentes variedades tales como: ataques contras datos informáticos, usurpación de la identidad, difusión de imágenes de agresión sexual contra

menores, estafas via internet, irrupción en servicios financieros, propagación de virus, botnets y phishing.

Dentro del código penal se encuentra la Ley 30096 “Ley de delitos informáticos” la cual se encuentra compuesta por siete capítulos, estos son:

Capítulo I. Finalidad y objeto de la ley

Capítulo II. Delitos contra datos y sistemas informáticos

Capitulo III. Delitos informáticos contra la indemnidad y libertad sexual

Capitulo IV. Delitos informáticos contra la intimidad y el secreto de las comunicaciones

Capitulo V. Delitos informáticos contra el patrimonio

Capítulo VI. Delitos informáticos contra la fe pública

Capitulo VII. Disposiciones comunes

Posterior a esto se promulgo la Ley 30171 (Ley que modifica la Ley 30096), esta ley busca adecuar la ley anterior a los estándares legales del convenio sobre la cibercriminalidad pronunciados en el Convenio de Budapest. Se modificaron los artículos 2,3,4,5,7,8 y 10 con el objetivo de garantizar las condiciones mínimas para el goce del derecho a la libertad y desarrollo. Con esta ley se busca hacer frente a la ciberdelincuencia y reducir los índices de inseguridad.

### **Bien jurídico tutelado**

Dentro de los delitos informáticos el bien jurídico tutelado es comprendido de una manera conjunta, donde se encuentra la información de manera general (información transmitida de datos) y en segundo plano los bienes afectados por delitos de indemnidad sexual, intimidad, etcétera. La información deber es aquella que contiene la base de datos o el producto de los procesos informáticos automatizados, es por la importancia del valor económico de la información que es incorporado dentro del bien jurídico tutelado.

Sin embargo, más allá del valor económico se debe considerar otras formas de afectación, por lo que en este tipo de delitos no solo se debe considerar la información como único bien jurídico afectado, sino como parte del conjunto de los bienes afectados.

### **Integridad personal**

Según Campomanes (2018) el concepto normativo y constitucional del derecho a la integridad, ha estado en constante evolución desde 1993, en la Constitución de 1979 del Estado Peruano se concretaba como derecho fundamental la integridad personal, tomando como único indicador la integridad física, aun no se integran daños de carácter psíquico y moral, ni se podía hacer uso de un Habeas Corpus para alegar los daños ocasionados.

Sin embargo, la Corte suprema en diferentes sentencias ha hecho referencia a considerar los daños psíquicos causados que afectan la integridad personal del individuo, así como también los diferentes tratos inhumanos que atentan y perjudican la conservación de la integridad personal como derecho humano establecido y reconocido a nivel internacional. Señala además la importancia del papel del Estado como ente fiscalizador y promotor de la conservación de la integridad personal, desarrollando diferentes estrategias para hacer frente a los diferentes tipos de delitos que atentan contra la integridad personal.

De acuerdo con Galindo (2009) el derecho a la Integridad personal ha sido un eje de trabajo de las Naciones Unidas a lo largo de los años, para lo cual se creó la Comisión de Derechos Humanos, el cual se encarga de evaluar el estudio de la tortura, de las penas crueles o inhumanas y toda actividad que amenace la integridad personal.

La Organización de los Estados Americanos muestra su preocupación por los distintos casos de desaparición y actos que vulneran la integridad de las personas, razón por la cual a nivel internacional se busca conservar la integridad física, moral y psíquica de toda persona. La integridad física implica la preservación de los órganos del cuerpo humano, así como el estado de salud en su totalidad. Por otro lado, la integridad psíquica hace referencia a la preservación de las habilidades motrices, emocionales e intelectuales. Por último, la integridad moral hace referencia a la libertad de cada individuo de desarrollar su vida acorde a sus preferencias y convicciones.

La vulneración al derecho de la integridad personal se ve afectado cuando concurren estos cuatro elementos:

- Elemento objetivo o material: existencia de actos que causen sufrimiento grave sobre la víctima
- Elemento subjetivo: que estén dirigidos por agentes del Estado en búsqueda de conseguir información de la persona.
- Calificación del victimario: las personas responsables de este actuar son los agentes del Estado o funcionarios públicos
- Condición de la víctima: las actividades realizadas pueden ser consideradas torturas dependiendo la condición del individuo.

La integridad personal se puede ver violentada de diferentes formas, entre las principales muestras se encuentran:

- La tortura
- Tratos o penas crueles, inhumanos o degradantes
- Detención arbitraria
- Lucha contra el terrorismo

### **Derecho a la intimidad personal**

Fayos (2015) menciona que el derecho a la intimidad personal consiste en la protección de la invasión de la información de la vida personal y familiar, para evitar la intromisión de terceros en contra de su voluntad. Por otro lado Carbonell (2006) señala la existencia de dos tipos de intimidad: la intimidad territorial y la intimidad informacional, donde se involucran los medios digitales o el ciber mundo en la actualidad.

## Definición de términos básicos

### Banco de datos

Es un conjunto de recopilación de información que nos permite llegar al conocimiento o deducir las consecuencias legítimas de un hecho, su representación es única e integrada y permite diversas utilidades. (Camps, y otros, 2005, p.2)

### Black hat

Es una persona que utiliza la tecnología o directamente referido el internet, con una destreza digital muy desarrollada la cual lo utiliza para de realizar hechos ilícitos. Se puede decir también que en otros países el BLACK HAT se conoce como las acciones incorrectas de las tecnologías (Francisco Canals, 2020, p. 01).

### Carding

Es la acción de realizar un hecho ilícito, en el implica realizar maniobras relacionadas con el duplicado de tarjetas, realizando movimientos para realizar todo tipo de acción para consumir todo el peculio que pueda tener la tarjeta, lo más cotidiano es la compra por internet (Francisco Canals, 2020, p. 01).

### Cibercrimen

Son todas las acciones ilícitas que se realizan de manera digital para obtener un tipo de beneficio, tienen como objeto realizar mediante herramientas digitales estos hechos contra organizaciones, empresas o gobiernos (Ciberseguridad, 2020, parr.4)

### Ciberseguridad

Es el conjunto de acciones, que tiene la condición característica, para la detección de riesgos y amenazas digitales, protegiendo todos los componentes lógicos, infraestructura digital, en busca la intangibilidad de ellos. (Ciberseguridad, 2020, parr.4)

### Datos informáticos

Es toda la representación de hechos, información y conceptos expresados de cualquier forma que se preste o tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. (Ley N° 30096, 2013, p. 3).

### Delitos informáticos

Es aquel término genérico utilizado para operación en contra de la ley, por medio del internet, teniendo como objetivos de dañar ordenadores, medios electrónicos y redes de internet, lo cual afecta a los bienes jurídicos de relevancias penales cometidas por medios tecnológicos. (Rendón, 2012, p. 12)

### Derechos fundamentales

Son aquellos derechos en el más alto lugar de protección jurídica, considerado por el poder constituyente como los más importante, Son los derechos humanos que son reconocidos por una norma fundamental es decir que se encuentran enmarcados dentro de un ordenamiento jurídico concreto de más alta jerarquía. (Rodríguez , 2018, p.148).

### Fraude informático

Es la actividad que mediante el uso de las tecnologías de información, procura para así o para terceros, el provecho ilícito en perjuicio de un individuo, que puede presentarse como cualquier interferencia o manipulación en el funcionamiento de un sistema informático (Ley N°30096, 2013, p.2).

### Interferencia telefónica

Es la actividad de interferir o escuchar una conversación por la vía telefónica, utilizando maniobras digitales de forma ilícita para la obtención de esa información (Ley N°30096, 2013, p.2).

### Ley 30096

Esta es una ley que tiene como objetivo de prevenir y sanciona todo tipo de actos de por medio de la tecnología, realiza maniobras que afectan sistemas y datos informáticos, mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de plantear un abordaje de forma correcta a este delito. (Ley N°30096, 2013, p.2).

### Hackers, crackers

Es toda persona que tiene un conocimiento elevado de cómo realizar maniobras digitales para tener todo tipo de acceso a cualquier portal virtual, de cualquier parte del mundo, no siempre esta adosado a hechos ilícitos; los Crackers a diferencia del hacker, se trata de una persona que si esta adosada a realizar hechos ilícitos, se puede decir que es un hacker, pero en versión negativa, tiene una connotación algo más ofensiva y delictiva. Realiza todo tipo de actividades que conlleva y conforman parte del cibercrimen. (Francisco Canals, 2020, p. 01).

### Interoperabilidad

Es la capacidad de interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos de todas las organizaciones, si tocamos el tema de sector público, de todas las instituciones. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información, procesos y las comunicaciones (PCM, 2012, p.71)

### Pharming

Es una modalidad de las personas que utilizan el medio tecnológico que se le puede llamar ciberdelincuentes, que buscan llegar a las cuentas bancarias de sus potenciales víctimas. Para esto se hace uso de páginas web falsas que suplantan a las originales (MININTER, 2016, p. 1)

### Suplantación de identidad

Es el uso de las herramientas tecnológicas para llegar a suplantación de identidad de una persona natural o jurídica, con objeto de tener algún beneficio para uno y perjuicio para otro, dicha acción adosada a lo ilícito ( Ley N°30096, 2013, p.2).

## CRONOGRAMA DE ACTIVIDADES

Actividades	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Producto Resultado
<b>1. Problema de la Investigación</b>													
1.1. Descripción de la realidad					X								
1.2. PI anteamiento del problema					X								
1.2.1. Problema General					x								
1.2.2. Problemas específicos													
1.3. Ob jetivos de la Investigación						x							
1.3.1. Objetivo General							X						
1.3.2. Objetivos Específicos													
1.4. Ju stificación e importancia de la investigación							x						
<b>2. Marco teórico</b>													
2.1. An tecedentes								X					
2.1.1. Internacionales								X					

2.1.2.Nacionales													
2.2. Ba ses teóricas									X				
2.3. De finición de términos									x				
<b>3. Conclusiones</b>									X				
<b>4. Recomendaciones</b>									X				
<b>5. Aporte científico o socio cultural de la investigación</b>									X				

Fuente: Elaboración propia.

## RECURSOS Y PRESUPUESTO

Partida Presupuestal*	Código de la actividad en que se requiere	Cantidad	Costo unitario (en soles)	Costo total (en soles)
Recursos humanos	Falta	1	300	
Bienes y servicios	Falta			
Útiles de escritorio	2. 3. 15	5	10	50
Mobiliario y equipos	2.3.22.2	1	500	500
Pasajes y viáticos	2.3.21.21	6	80	480
Materiales de consulta (libros, revistas, boletines, etc.)	2. 3. 15	10	20	200
Servicios a terceros	2.3.22.44	1	300	300
Otros				
Total				

Fuente: Elaboración propia.

## REFERENCIAS

- Andina. (16 de Enero de 2020). *Actualidad*. Obtenido de Estos son los delitos informáticos más frecuentes en el Perú, según la Policía: <https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx>
- Calderon, I. C. ( 2015). *Vacio legales que imposibilitan la sancion de ls delitos informaticos en el nuevo codigo penal peruano - 2015*. Lima, Peru: Universidad de Huanuco.
- Campomanes, R. (2018). *El derecho fundamental a la integridad personal: Física, psiquica y moral*. Lima: Pontificia Universidad Católica del Perú.
- Camps, R., Casillas, L., Costal, D., Gibert, M., Escofet, C., & Perez, O. (2005). *Base de Datos*. Barcelona, España: Universitat Oberta de Catalunya.
- Carbonell. (2005). *Teoría constitucional y derecho fundamentales*. Mexico: Porrúa.
- Chavez, E. (2017). *El delitos contra datos y sistemas de informacion en el derecho fundamental a la intimidad personal en la corte superio de justicia de Lima Norte, 2017*. Lima, Peru: Universidad Nacional Federico Villarreal.
- Chávez, E. (2018). *El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de Lima Norte* . Lima: Universidd Federico Villarreal.
- Chilcon, M. (2019). *El Ciber Crimen en el Peru y su incidencia en la Seguridad Nacional*. Lima, Peru.: Centro de Altos Estudios Nacionales.
- CiberSeguridad. (01 de 03 de 2020). *Ciberseguridad*. Obtenido de Glosario: <https://www.ciberseguridad.gob.cl/glosario/>
- CRUZ, C. A. (2016). *ANALISIS DE DELITOS INFORMATICOS Y SU VIOLACION DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS*. Loja - Ecuador: Universidad Nacional de Loja.

Diario El País. (28 de 01 de 2020). *Página 12*. Recuperado el 29 de 01 de 2020, de <https://www.pagina12.com.ar/244142-que-dicen-los-patovicas-sobre-el-crimen-de-villa-gesell>

Diario Hoy. (20 de 01 de 2020). *Diario Hoy Digital*. Recuperado el 29 de 01 de 2020, de <https://hoy.com.do/gonzalo-castillo-seguira-fortaleciendo-las-politicas-de-seguridad-ciudadana-de-rd-afirma-jose-ramon-peralta/>

Echevarria, G. (2015). *Delitos Informaticos y el Derecho Constitucional a la seguridad publica*. Ambato, Ecuador: Universidad Tecnica de Ambato.

Eduardo, V. C. (s.f.). LOS DELITOS INFORMATICOS Y SIU.

Fayos. (2015). *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Madrid: Dykinson SL.

Francisco Canals periodista. (2020). *Diccionario de Delitos Ciberneticos*. Barcelona, España: <http://www.fcanals.com/diccionario-de-delitos-ciberneticos/>.

Galindo, J. (2009). Contenido del derecho a la integridad personal. *Derecho del Estado N°23*, 90-125.

Guerrero, L., & Santiago, A. (2013). El uso legítimo de la fuerza policial: Breve acercamiento al contexto mexicano. *Ciencia Jurídica Vol.1 N°3*, 31.

Guillen, F. (2015). *Modelos de policia y seguridad*. Barcelona, España: Universidad Autonoma de Barcelona.

INTERPOL. (2013). *INTERPOL*. Obtenido de INTERPOL: <https://www.interpol.int/es/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia>

kierszenbaum. (2009). El Bien jurídico en el derecho penal. *Lecciones y Ensayos N°86*.

Lopez, D. F. (2014). *Los Delitos informaticos y la violacion de los derechos constitucionales del ofendido*. Ambato, Ecuador: Universidad Tecnica de Ambato.

- Machaca, J. (2018). *Análisis de la influencia del cyberbullying en la integridad personal y su implementación dentro de los delitos informáticos en la legislación peruana - Arequipa*. Arequipa - Peru: Universidad Autónoma San Francisco.
- Maldonado, M. (s.f.). *El Delito Informático, vulnera el principio de la garantía constitucional y legal, sobre el honor de las personas establecidos en la constitución de la República*. Loja, Ecuador: Universidad Nacional de Loja.
- Maldonado Ortega, M. D. (2014). *El Delito Informático, vulnera el principio de la garantía constitucional y legal, sobre el honor de las personas establecidos en la constitución de la República*. Loja, Ecuador: Universidad Nacional de Loja.
- Maldonado, E. (2016). *Los Delitos Informáticos y el Derecho Constitucional a la Seguridad Jurídica*. Babayoho, Ecuador: Universidad Regional Autónoma de Los Andes.
- Maya, R. (2014). *Delitos Contra la vida y la integridad personal*. Medellín, Colombia: Grupo Editorial Ibañez.
- Mera, G. A. (2015). *Los Delitos Informáticos y el Derecho Constitucional a la Seguridad Pública*. Ambato, Ecuador: Universidad Técnica de Ambato.
- MININTER. (2016). *Ciber Policías contra los Delitos Informáticos*. Lima, Peru: Oficina de Comunicación Social.
- MPFN. (2019). *Boletín Estadístico del Ministerio Público*. Lima, Peru: Ministerio Público Fiscalía de la Nación.
- Narvaez, B., & Recalde, G. (2018). *El Delito Informático en América*. Quito, Ecuador.: Uniandes Revista Jurídica.
- (2013). *Necesidad de precautelar la garantía constitucional establecida en el art 66 numeral 3 literal A que se garantiza la integridad, física, moral o sexual que se vulneran por el delito informático*. Loja, Ecuador: Universidad de Loja.
- Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). *Metodología de la investigación*. Bogotá, Colombia: Ediciones de la U.

- PCM. (2012). *Plan Nacional de Gobierno Electrónico 2013-2017*. Lima, Perú: Oficina Nacional de Gobierno Electrónico e Informática - ONGEI.
- Perfil. (29 de Enero de 2020). *OPINIÓN / COLUMNA DE LA USAL*. Obtenido de El Ciberespacio, fuente de amenazas a la seguridad, y el desafío de Naciones Unidas: <https://www.perfil.com/noticias/opinion/opinion-mariano-bartolome-el-ciberespacio-fuente-de-amenazas-a-la-seguridad-y-el-desafio-de-naciones-unidas.phtml>
- Pizarro, V. M. (2019). *Repercusión de la policía nacional del Perú y el cumplimiento de la ley N° 27933 en el distrito de Huánuco*. Huánuco, Perú: Universidad de Huanuco.
- Posada, R. (2017). *Los Cibercrímenes*. Medellín, Colombia: Grupo Editorial Ibañez.
- Rendon, D. (2012). *La eficacia de la prueba digital en el proceso penal colombiano*. Medellín, Colombia: Católica del Norte Fundación Universitaria.
- Rodríguez, E. G. (2017). *El Delito Contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de corte superior de justicia Lima Norte, 2017*. Lima, Peru: Universidad Federico Villareal.
- Ruiz, C. (2016). *Análisis de los Delitos Informáticos y su violación de los derechos constitucionales de los ciudadanos*. Loja, Ecuador: Universidad Nacional de Loja.
- Silva, M. C. (2019). *El Cibercrimen en el Perú y su incidencia en la seguridad ciudadana*. Lima, Peru: CAEN.
- Silvestre, I., & Huamán, C. (2019). *Pasos para elaborar la investigación y redacción de la tesis universitaria*. Lima, Perú: Editorial San Marcos.
- Temperini, M. (2013). *Delitos Informáticos en Latinoamérica*. Buenos Aires, Argentina: Universidad Nacional del Litoral.

- Tocto, K. J. (2018). *Inconsistencias y ambigüedades en la Ley de delitos informáticos ley N° 30096 y su modificatoria Ley N° 30171 , que imposibilitan su eficaz cumplimiento*. Huaraz, Peru: Universidad Nacional de Ancash "Santiago Antiguos de Mayolo".
- Trejo, C., Domenech, G., & Ortiz , K. (2015). *La Seguridad Jurídica frente a los Delitos Informáticos*. Cajamarca, Peru: AVANCES, revista de investigación jurídica.
- Uribe, E., & Flores, A. (2013). La naturaleza constitucional dual de la seguridad pública. *Revista In Jure Anáhuac Mayab Vol 2 N° 3; ISSN 2007-6045*, 39-55.
- USCG. (2014). *La Seguridad de la Información*. Guatemala: Universidad San Carlos de Guatemala.
- Valderrama, S. (2019). *Pasos para elaborar proyectos y tesis de investigación*. Lima, Perú: San Marcos.
- Velastegui Cordova, M. E. (2019). LOS DELITOS INFORMATICOS Y SU INCIDENCIA EN LA PROVINCIA DE PASTAZA. *Revista digital de ciencias jurídicas de UNIANDES*, 45-49.
- Villavicencio. (2014). Delitos informáticos. *IUS VERITAS*.

## **APORTE CIENTÍFICO O ACADÉMICO**

El aporte académico de esta investigación se manifiesta por el alto dato de hecho ilícitos, los cuales se realizan por el uso de la tecnología con maniobras direccionadas a una fin ilícito, este tema es de interés público y de alta importancia para la comunidad académica los cuales también son un margen potencial como futuras víctimas, por tal motivo están interesados en conocer y profundizar en temas de seguridad ciudadana y tomando en cuenta una seguridad jurídica en tecnologías, con un fin de bienestar social, para esta investigación se busca detectar en cuanto afecta los delitos informáticos a la integridad personal, ya que no solo se habla de una afectación al patrimonio de una persona, sino a la honorabilidad, etc. Se buscará determina la incidencia de la actividad ilícita en el distrito de Chorrillos como localidad elegida, esto para combatir la criminalidad, siendo un tema novedoso por lo poco investigado por ser un tema donde entra a tallar la tecnología teniendo una perspectiva científica, rigor académico y estadístico dentro del ámbito profesional de la carrera de derecho, contribuirá a futuros profesionales interesados en profundizar en los hallazgos planteados en esta investigación.

## RECOMENDACIONES

Se recomienda al Ministerio Público, posibilite a nivel nacional plantear estrategias para que se realicen frecuentes actividades de capacitación en materia al abordaje a estos delitos informáticos que paran en constante cambio y fomentar una convivencia en paz, en bienestar de la población.

Se recomienda a poderes gubernamental dar la herramienta correspondiente a los operadores de justicia para que así se pueda enfrentar a esta organización que son peritos en maniobras digitales y actúan de forma internacional y con toda la tecnología permanente.

Se recomienda al ejecutivo repotenciar a la dirección de delitos informáticos para que este al nivel correspondiente y pueda enfrentar estos actos de forma eficiente y eficaz, con resultados positivos.

Así mismo los gobiernos locales en sus planes de desarrollo de su gestión, deben plantear programas de prevención de estos delitos para minimizar el analfabetismo digital, que es el primer factor para que se realice un hecho ilícito con el uso indebido de la tecnología.

## ANEXOS

## Cuestionario N° 1: Delitos informáticos

## Atención:

Un cordial saludo, en esta oportunidad solicito a usted completar el presente cuestionario, el cual pertenece a un estudio con fines estrictamente académicos. Se muestra una escala de valoración para su respectivo llenado por cada ítem propuesto. Agradeceré marcar con un aspa (X) en cada uno de los ítems mencionados, colocando una sola respuesta en cada uno. Muchas gracias.

La escala de medición utilizada para el llenado de sus respuestas:

Escala de Valoración (Likert)				
Nunca	Casi Nunca	A veces	Casi Siempre	Siempre
1	2	3	4	5

Marcar en una de las siguientes casillas, según corresponda:

N°	Descripción del ítem	Escala de Valoración				
		1	2	3	4	5
<b>Delitos informáticos contra la indemnidad y libertad sexual</b>						
1	En algún momento, ha sido contactado para brindar contenido que atente contra su libertad sexual					
2	En algún momento, ha sido contactado para realizar actividades sexuales contra su seguridad y libertad sexual					
3	En algún momento, ha recibido sin solicitarlo material pornográfico contra su indemnidad y libertad sexual					
<b>Delitos informáticos contra la intimidad y el secreto de las comunicaciones</b>						
4	Ha padecido el uso indebido de información que atente contra su intimidad personal					
5	Ha sufrido interceptación de datos informáticos que atenten contra su intimidad personal					
6	Ha sido contacto por terceros sin solicitar previamente información por los bienes y/o servicios que le ofertan					
<b>Delitos informáticos contra datos y sistemas informáticos</b>						
7	Ha conocido sobre hechos realizados por terceros que han accedido de manera ilícita a sistemas informáticos					
8	Ha accedido sin autorización a algún sistema de información de terceros o de su centro laboral					
9	Se ha visto afectado por actos ilícitos de los sistemas de información que maneja en su centro de trabajo o de manera personal					
<b>Delitos informáticos contra el patrimonio</b>						
10	Ha conocido sobre hechos realizados por terceros que han afectado de manera ilícita el patrimonio de terceros					
11	Ha sido perjudicado y/o afectado por terceros en provecho ilícito de su patrimonio de negocio o sociedad					

12	Ha sido perjudicado y/o afectado por terceros en provecho ilícito de su patrimonio personal					
	<b>Delitos informáticos contra la fe pública</b>					
13	Su identidad como persona natural se ha visto suplantada en alguna oportunidad					
14	Su identidad como persona jurídica se ha visto suplantada en alguna oportunidad					
15	Ha sido perjudicado y/o afectado por la suplantación de identidad					

## Cuestionario N° 2: Integridad personal

### Atención:

Un cordial saludo, en esta oportunidad solicito a usted completar el presente cuestionario, el cual pertenece a un estudio con fines estrictamente académicos. Se muestra una escala de valoración para su respectivo llenado por cada ítem propuesto. Agradeceré marcar con un aspa (X) en cada uno de los ítems mencionados, colocando una sola respuesta en cada uno. Muchas gracias por el apoyo brindado.

La escala de medición utilizada para el llenado de sus respuestas:

Escala de Valoración (Likert)				
Nunca	Casi Nunca	A veces	Casi Siempre	Siempre
1	2	3	4	5

Marcar en una de las siguientes casillas, según corresponda:

N°	Descripción del ítem	Escala de Valoración				
		1	2	3	4	5
	<b>Integridad física</b>					
1	Ha sido contactado por terceros que atenten contra su integridad física a través de medios informáticos					
2	Ha conocido casos de familiares o conocidos, cuya integridad física haya sido afectada					
3	Ha reportado alguna situación que comprometa su integridad física a través de medios informáticos					
4	Ha sufrido violencia física en medios informáticos					
	<b>Integridad psíquica</b>					
6	Ha sido contactado por terceros que atenten contra su integridad psíquica a través de medios informáticos					
7	Ha conocido casos de familiares o conocidos, cuya integridad psíquica haya sido afectada					
8	Ha comunicado alguna situación que comprometa su integridad física a través de medios informáticos					
9	Ha sufrido violencia psíquica en medios informáticos					
	<b>Integridad moral</b>					
11	Ha sido contactado por terceros que atenten contra su integridad moral a través de medios informáticos					
12	Ha conocido casos de familiares o conocidos, cuya integridad moral haya sido afectada a través de medios informáticos					

13	Ha reportado alguna situación que comprometa su integridad física a través de medios informáticos					
14	Ha sufrido violencia moral en medios informáticos					