FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogado

AUTORES:

Adarmes Alvarez, Leopol Martin (ORCID: 0000-0002-0008-5663)

Ortiz Cahuana, Andy Antonio (ORCID: 0000-0001-6098-4249)

ASESORA:

Mgtr. Palomino González, Lutgarda (ORCID: 0000-0002-5948-341X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

LIMA – PERÚ

2020

Dedicatoria

A Dios; a mis padres, Oscar y Angelica, mis hermanos y mi familia, a mi asesora de tesis, Lutgarda, por su paciencia y dedicación como docente en esta etapa final de la carrera.

Andy Antonio Ortiz Cahuana

A mi padre, Leopoldo Santiago Adarmes Gamarra, que desde la eternidad me guía, cuida y protege a mi familia, gracias por todo.

Leopol Martin Adarmes Alvarez

Agradecimiento

Agradezco a la universidad Cesar Vallejo, a mis maestros por sus esfuerzos para que finalmente me pudiera graduar con éxito.

Andy Antonio Ortiz Cahuana

A la universidad, mis docentes, mis asesores que me vieron desde el inicio, y ahora con mucha alegría también me verán graduarme.

Leopol Martin Adarmes Alvarez

Índice de contenidos

Índice de tablas

Pág.

Índice de gráficos y figuras

Resumen

La investigación tiene por finalidad identificar las intervenciones de los operadores de justicia hacía el aumento de amenazas de delitos informáticos que, durante el inicio del estado de emergencia sanitaria, así como la inmovilización social obligatoria por COVID -19, hasta el día de hoy afecta a miles de peruanos, que se ven desprotegidos por la administración de justicia.

El problema de la investigación fue ¿existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19? El objetivo de la investigación fue identificar la intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19. Para concretar la presente investigación se tuvo un enfoque cualitativo, tipo básico con el diseño de la teoría fundamentada, así también métodos de investigación como el instrumento de recolección de datos aplicados a diferentes profesionales involucrados en el tema, para así permitir el reconocimiento de la intervención de los operadores de justicia a la amenaza del delitos informáticos, encontrándose en ello discrepancias, coincidencias, pues también se interpretó en base a sus ideas centrales. Finalmente se concluyó que no nos encontramos en la capacidad jurídico-penal, para hacer frente a ello, de igual forma se descubrió la interpretación de la administración pública a estos delitos como un medio para llegar al mismo dentro del cuerpo penal, mas no del propio delito ya iniciado, teniéndose en cuenta la ley especial 30096 (Ley de delitos informáticos).

Palabras clave: operadores de justicia, delitos informáticos, estado de emergencia, covid-19.

Abstract

The purpose of the investigation is to identify the investments of justice operators towards the increase in threats of computer crimes that, during the beginning of the state of health emergency, as well as the mandatory social immobilization due to COVID -19, to date affects thousands of Peruvians, who are unprotected by the administration of justice.

The problem of the investigation was, is there intervention of justice operators in the face of the increase in threats of computer crimes during the state of emergency due to covid-19? The objective of the investigation was to identify the intervention of justice operators in the face of the increase in cybercrime threats during the state of emergency due to covid-19. To carry out the present research, a qualitative approach was taken, a basic type with the design of the grounded theory, as well as research methods such as the data collection instrument applied to different professionals involved in the subject, in order to allow the recognition of the intervention from justice operators to the threat of cybercrime, finding discrepancies, concurrence, as they will also be interpreted based on their central ideas. Finally, it was concluded that we are not in the legal-criminal capacity to deal with it, in the same way, the interpretation of the public administration to these crimes was discovered as a means to reach the same within the criminal body, but not the own crime already started, taking into account special law 30096 (Law of computer crimes).

Keywords: justice operators, cybercrime, state of emergency, covid-19

I. INTRODUCCIÓN

En el presente capítulo se presenta la realidad mundial y nacional acerca de la intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19, el propósito de este capítulo es pues describir la evidente amenaza que supone el delito informático en estas temporadas que, por cuarentena, las personas están utilizando en mayor cantidad de tiempo sus computadora o dispositivos móviles.

Durante la pandemia de COVID-19, los delincuentes se apresuraron a aprovechar las oportunidades para explotar la crisis adaptando su modus operandi y participando en nuevas actividades criminales. Los cibercriminales han estado entre los más expertos en explotar la pandemia. La amenaza de las actividades de delitos informáticos durante la crisis es dinámica y tiene el potencial de aumentar aún más. Con un número récord de víctimas potenciales que se quedan en casa y utilizan los servicios en línea en todo el mundo, en tal sentido, las formas para los ciberdelincuentes que buscan explotar las oportunidades y vulnerabilidades emergentes se han multiplicado (Gómez, 2020).

Antúnez (2020) explicó que los delitos informáticos van desde vender curas falsas de coronavirus en línea hasta un ciberataque en los sistemas de información crítica de los hospitales, los delincuentes están explotando la crisis COVID-19. En tiempos de crisis, la ciberseguridad es de importancia crítica, ya que una gran cantidad de personas bajo restricción o restricciones de movimiento ahora trabajan y estudian de forma remota, lo que los hace susceptibles a los delitos informáticos a través de correos electrónicos de phishing con archivos adjuntos y enlaces.

Una de las medidas preventivas clave para la propagación de Covid-19 es el distanciamiento social. Afortunadamente, en este mundo cada vez más conectado, podemos continuar virtualmente nuestra vida profesional y privada. Sin embargo, con grandes aumentos en el número de personas que trabajan de forma remota, es de vital importancia que también cuidemos nuestra “salud” cibernética (De Pedro, 2020).

Bezuidenhout et al. (2010) explicaron que en un mundo donde abunda el pánico y la necesidad de sentirse informado, proporciona a los cibercriminales una

plataforma masiva de víctimas desprevenidas. La ingeniería social está en su apogeo en este momento, ya que se aprovecha de las personas que se encuentran en un estado emocional elevado.

Mouton et al. (2014) delimitó que: “es la ciencia del uso de la interacción social como un medio para persuadir a un individuo para que cumpla con una acción específica de un atacante donde la interacción involucra una entidad relacionada con la computadora”. (p. 1).

Durante los últimos días se ha decretado el estado de emergencia en muchos países llegando incluso a hacer efectivo el toque de queda para los ciudadanos, se ha visto también que la mayoría de las empresas solicitaron a su fuerza laboral que trabaje desde su hogar cuando sea posible. Varios países, como Italia y España, se han visto obligados a permanecer encerrados. Esto ha provocado que las personas se vuelvan totalmente dependientes de la tecnología para la comunicación, las noticias, el entretenimiento y la interacción social (Tarun, 2020).

El delito informático a pesar de estar presente en la Ley N°30096 y en el Código Penal del Perú, no es explícita ya que, según el objeto de esta ley, tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, sin embargo, no presenta la especificación y castigo para los delitos informáticos más comunes como lo son: Phishing, URL's falsas, ataques a los sistemas físicos, grooming, revelación de secretos e infodemia (Otárola y Luna, 2014).

La justificación teórica de esta investigación se encuentra en la formulación de conocimiento para complementar el vacío existente en la Ley N° 30096 sobre los delitos informáticos, para que de esta manera se pueda generalizar los resultados a principios más amplios, lo que en gran medida mejorará la intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos.

La justificación social de este estudio está explicita en el beneficio de manera principal, a aquellas personas que han sido víctimas de los delitos informáticos y que no han encontrado respuesta en los órganos judiciales precisamente por no encontrarse explícito cada una de los “modus operandi” de la ciberdelincuencia, además beneficia a los operadores de justicia ya que permitirá la expansión de los

conocimientos para lograr una buena respuesta judicial ante esta creciente amenaza.

La justificación metodológica de esta investigación está fundada en buscar establecer la importancia de definir de manera perfecta el concepto de los delitos informáticos y sus modus operandi en el Decreto Legislativo N° 957 Código Procesal Penal (Gobierno del Perú, 2004).

La justificación práctica de esta investigación está en las implicaciones trascendentales que otorgará la clara delimitación de los delitos informáticos que apoyará a que la intervención de los operadores de justicia ante esta creciente amenaza sea eficiente.

Sobre la base de la realidad problemática presentada se planteó el problema general y los problemas específicos de la investigación. El problema general de la investigación fue: ¿existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19? Los problemas específicos de la investigación fueron los siguientes:

- **P.E. 1:** ¿Existe un déficit normativo en la Ley de delitos Informáticos que debilita la intervención de los operadores de justicia?
- **P.E. 2:** ¿Hay un perfil para el reconocimiento por parte de los operadores de justicia del modus operandi en la comisión de un delito informático?
- **P.E. 3:** ¿Existía intervención de los operadores de justicia a las amenazas de delitos informáticos antes del estado de emergencia por covid-19?

El objetivo general fue identificar la intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19. Los objetivos específicos fueron los siguientes:

- **O.E. 1:** Demostrar la existencia del déficit normativo de la Ley de Delitos Informáticos que debilita la intervención de los operadores de justicia en los delitos informáticos.
- **O.E. 2:** Configurar el perfil para el reconocimiento por parte de los operadores de justicia del modus operandi en la comisión de un delito informático.

- **O.E. 3:** Establecer la intervención de los operadores de justicia a las amenazas de delitos informáticos antes del estado de emergencia por covid-19.

II. MARCO TEÓRICO

Este segundo capítulo del trabajo de investigación abordará los antecedentes nacionales e internacionales de relevancia para el tema de investigación, los mismos que fueron seleccionados según el criterio de las variables referido a la intervención de los operadores de justicia ante los delitos informáticos. Además, también se presentarán las teorías relacionadas a esta problemática que servirá como el sustento teórico de la investigación. Posteriormente se presentarán algunos conceptos claves que son necesarios conocer para entender el fenómeno de los delitos informáticos.

A continuación, se presentarán los antecedentes nacionales e internacionales de la investigación, por tratarse de un campo fusionado entre el derecho y la tecnología, no existen muchas fuentes que precisen la comisión del delito en la modalidad de los delitos informáticos, sin embargo, se plantean estudios relacionados a las amenazas a la seguridad de la información y otros que indagan los delitos informáticos de manera directa.

Beteta et al. (2018) estudiaron la preparación de Mapfre Perú Seguros y Kallpa Corredora de Seguros, ante las amenazas de seguridad de la información. Beteta et al. (2018) tomaron como muestra a autoridades fundamentales de la seguridad de la información de Mapfre Perú y Kallpa. Beteta et al. (2018) hallaron que este tipo de organizaciones debe asegurar también la seguridad de la información bajo el concepto de “Insurtech” (tecnología de seguros). Beteta, et al. (2018) concluyen que en materia de seguridad de la información sólo se establecen normativas que no son actualizadas y son de suma importancia. Finalmente, Beteta et al. (2018) recomiendan que se debe adoptar controles de ciberseguridad para que la información no sea vulnerada.

Alarcón y Barrera (2017) estudió la determinación de la relación del uso del internet y los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia. Alarcón y Barrera (2017) definieron que su muestra estuvo conformada 60 estudiantes pertenecientes al primer semestre de pregrado. Alarcón y Barrera (2017) hallaron que el uso del internet mediante las competencias informacionales se relaciona con los delitos informáticos de derecho de autor. Alarcón y Barrera (2017) concluye que el uso

legal de la información y el uso correcto de las redes sociales depende del desarrollo de competencias. Finalmente, Alarcón y Barrera (2017) recomiendan abrir espacios de capacitación en las normas legislativas e institucionales.

Quevedo (2017) buscó estudiar la trascendencia existente en el uso de internet en la aparición de nuevos ciberdelitos. Quevedo (2017) toma como muestra el estudio de las cuestiones básicas de los ciberdelitos. Quevedo (2017) halló que el ciberdelito son todas las conductas sancionadas por el Código Penal y las posibles conductas aún no tipificadas. Quevedo (2017) concluye que es necesario definir al ciberdelito y distinguirlo "stricto sensu" de aquellos delitos clásicos de medio comisivo. Quevedo (2017) recomienda que cuando el ciberdelito es cometido se debe reconocer la competencia absoluta para su persecución a favor del Juez y de todos los organismos judiciales sobre los lugares donde se manifiesten los efectos del ciberdelito.

Cajamarca (2016) estudió la implementación de un laboratorio de informática forense en el órgano rector del Sistema de Inteligencia Nacional. Cajamarca (2016) utilizó como muestra las instalaciones del órgano rector del Sistema de Inteligencia Nacional con la participación del personal policial y militar que componen al órgano mencionado. Cajamarca (2016) halló que el 53% de las empresas peruanas a las que evaluaron admitieron tener poca capacidad para detectar un ataque sofisticado. Cajamarca (2016) concluye que, los dispositivos no solo registran una gran cantidad de información personal. Finalmente, Cajamarca (2016) recomienda realizar un adecuado análisis forense informático requiere de un equipo multidisciplinar que incluya profesionales expertos.

Larios y Sánchez (2014) buscaron brindar un panorama de lo que representa la seguridad de la información a través de los servicios de internet. Larios y Sánchez (2014) utilizaron una muestra comprendida por revisión sistemática de la literatura a través de la cual pudieron definir conceptos base y relevantes para la constitución del fundamento teórico Larios y Sánchez (2014) hallaron que el modelo de Baran es una de las figuras clave para la creación de internet. Larios y Sánchez (2014) llegaron a la conclusión de que las tecnologías de la información han sido adaptadas y utilizadas como herramientas para infringir la ley. Larios y Sánchez

(2014) recomiendan que se debe tener especial cuidado con los correos, ofertas e incluso hasta con las llamadas telefónicas.

González (2013) investigó la regulación de delitos relacionados con nuevas tecnologías que no han tenido precedentes. González (2013) utilizó la revisión sistemática y el análisis de los datos hallados en el código penal español. González (2013) halló que se ha desarrollado bastantes sistemas y programas de seguridad pero que no impiden surgimiento de nuevas formas de criminalidad. González (2013) concluye que no hay una correcta determinación del bien jurídico protegido por los delitos de daños informáticos. González (2013) recomienda que se debe crear un núcleo fácilmente reconocible en el derecho penal para así desprenderse del proceso en el cual la legislación no se ha detenido especialmente en la concepción de la ciberdelincuencia.

Según los antecedentes propuestos, es necesario construir un sustento teórico donde se conozca la base teórica de este trabajo de investigación, por lo tanto, se investigaron los conocimientos teóricos más fundamentales que complementan a la investigación.

El phishing es probablemente el elemento número uno que ha experimentado un aumento masivo durante estos tiempos difíciles. La sociedad tiene hambre de información, o incluso de algún tipo de alivio, y por lo tanto el phishing es mucho más exitoso durante estos tiempos. La mayoría de los ejemplos que se han visto en la naturaleza son los correos electrónicos, como las autoridades fiscales que ofrecen "reembolsos de impuestos” para ayudarlos a enfrentar la pandemia del covid-19. Todo lo que tenían que hacer era ingresar su nombre, dirección, número de teléfono, apellido de soltera de la madre y número de tarjeta bancaria, una estafa clara. Los atacantes cibernéticos también siguen muy de cerca las tendencias y noticias mundiales (Hadnagy 2018).

Durante el mes pasado se produjo un aumento masivo en la adquisición de URL falsas, asociadas a COVID-19). Por lo general, el modus operandi es para que los scammers puedan recoger un montón de dominios relacionados con COVID-19 y convertirlos en sitios de inyección de malware malicioso. Después de que se hayan tomado todos los dominios 'buenos', los estafadores eventualmente comenzarán a

aprovecharse de los dominios que contienen errores tipográficos, usando palabras como 'coronovirus' en lugar de 'coronavirus' (Grossman, 2020).

Algunas páginas que incluyen el nombre corona son los siguientes: corona-emergency.com, combatcorona.com, buycoronavirusfacemasks.com, beatingcorona.com, coronadetection.com, coronadatabase.com. Esto muestra claramente que este proceso está en curso continuo y que las personas deben estar en busca de URL falsas. Es lamentable que, en una situación de histeria masiva, las buenas URL, como "beatingcorona" (Venciendo al coronavirus) o "coronadetection" (Detección de coronavirus) ya hayan sido tomadas por personas con intenciones maliciosas. Estas URL podrían haberse utilizado con buenos propósitos, permitiendo a las personas localizar fácilmente la información correcta y precisa (AT&T, 2020).

Por lo general, cuando se habla del panorama de amenazas de seguridad cibernética, las personas a menudo olvidan los ataques físicos que aún tienen lugar. Estos tipos de ataques aún dependen de la ingeniería social, sin embargo, se basan en el simple hecho de que las personas ya están en un estado de histeria y necesitan asistencia de algún tipo. Una de las agencias de seguridad física ha informado que hay individuos que presentan como "samaritanos" y ofrecen a las personas máscaras faciales gratuitas, desinfectante para manos y otros productos cuyos suministros se han reducido durante la crisis del coronavirus. Utilizando esta técnica, los "samaritanos" están obteniendo acceso físico a los hogares de las víctimas (Morrison, 2020).

La otra técnica son los individuos que se hacen pasar por “samaritanos” que pueden ayudar a desinfectar su hogar. Estas personas luego solicitan acceso a su hogar, ya que necesitan rociar productos químicos en la casa y pedirle que espere afuera mientras este proceso es sucediendo. En ambos casos, los ciberdelincuentes se aprovechan de la idea de que las personas tienen miedo y tienen la necesidad inherente de mantenerse a salvo. La noción de permanecer seguro actualmente es usar productos de limpieza y garantizar que su hogar esté limpio (Herman y Henry, 2020).

También ha habido un aumento masivo de personas que inician páginas web de donaciones donde las personas pueden donar para ayudar a los investigadores a encontrar la cura para COVID-19.Las personas

son inherentemente buenas y siempre quieren ayudar, y por lo tanto los ingenieros sociales se aprovechan del mero hecho de que las personas quieren ayudar a sus compatriotas perdonando a la causa. En la mayoría de estos casos, estas páginas de donación en realidad no se administran correctamente y, por lo general, solo el individuo que aloja la donación se beneficia de la campaña de donación (Nelson, 2020).

Es sumamente preocupante que actualmente sea uno de los mejores momentos para revelar los datos privados de una agenda personal durante estos tiempos difíciles. Varias personas están tratando de obtener ganancias de esto mediante el almacenamiento de productos y eventualmente tratando de revender los productos a un valor mucho mayor (BBC News, 2020a). Afortunadamente, varios gobiernos han puesto fin a esto y la ley prohíbe el aumento de precios (Department of Justice Delaware, 2020). El gobierno también está actuando contra personas que intentan promocionar sus propios productos, como un presentador de radio que promovió que su marca de pasta dental podría curar COVID-19 (Ferre-Sadurni & McKinley, 2020).

La información errónea o infodemia es uno de los mayores enemigos de la sociedad durante esta pandemia. Dado que el público está haciendo un trabajo espectacular al compartir noticias sensacionales falsas entre ellos, los ciberdelincuentes solo deben publicar las noticias de manera sensacional. Ha habido un flujo masivo de nuevos artículos falsos y varias compañías están tratando activamente de resolver esto (BBC News, 2020b).

Uno de los primeros ciberataques relacionados con COVID-19 fue con respecto a los mapas falsos de COVID-19. La Universidad Johns Hopkins proporcionó uno de los primeros mapas que incluía estadísticas para el mundo. Este ha sido un gran recurso para la sociedad y ha demostrado ser enormemente beneficioso. Sin embargo, como era tan popular, los ciber atacantes crearon sus propias versiones "falsas" del sitio web que requerían que descargaras un complemento. Este

complemento permitiría a su vez a un atacante obtener acceso remoto a su sistema (Fowler & Duncan, 2020).

El grooming o acoso cibernético es el proceso de "hacerse amigo" de un menor de edad en línea "para facilitar" el contacto sexual en línea y / o una reunión física con ellos con el objetivo de cometer abuso sexual. El acoso cibernético es cuando alguien (a menudo un adulto) se hace amigo de un niño en línea y construye una conexión emocional con futuras intenciones de abuso sexual, explotación sexual o tráfico. Los objetivos principales del acoso cibernético son: ganar la confianza del niño, obtener datos íntimos y personales del niño (a menudo de naturaleza sexual) para amenazar y chantajear por material inapropiado adicional (Ortigosa y Hernández, 2016).

El Protocolo de Asistencia Jurídica Mutua en Materia Penal —También conocido como el Protocolo de San Luis— registra en sus fundamentos que la cooperación en materia jurídica favorece a lograr aumentos en el sentimiento de profundidad sobre la reciprocidad de intereses de los Estados Parte en el proceso de integración. Además, este Pacto refiere que la respuesta colectiva es necesaria por la grave inminencia que se manifiesta a través de modalidades criminales transnacionales. Su objeto radica en regular la cooperación en materia de recepción y producción de prueba (documentos, testimonios, peritajes, registros, etc.), los procedimientos particulares y ejecuciones jurídicas (Deluca y Carril, 2017).

Contreras (2003) define que el bien jurídico protegido, según la historia fidedigna de la ley contra los delitos informáticos en Chile es la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de esta y de los productos quede su operación se obtengan.

Los delitos informáticos es cualquier actividad criminal que involucra un dispositivo en red o una red. Si bien la mayoría de los delitos cibernéticos se llevan a cabo con el fin de generar ganancias para los delincuentes cibernéticos, algunos delitos cibernéticos se llevan a cabo contra computadoras o dispositivos directamente para dañarlos o desactivarlos, mientras que otros usan computadoras o redes para difundir malware, información ilegal, imágenes u otros materiales (Barnor y Patterson, 2020).

De la misma manera, si existe un delito informático, existirán cibercriminales, los cuales son también conocidos como piratas informáticos, a menudo utilizan sistemas informáticos para obtener acceso a secretos comerciales e información personal con fines maliciosos y de explotación. Los hackers son extremadamente difíciles de identificar tanto a nivel individual como grupal debido a sus diversas medidas de seguridad, como los servidores proxy y las redes de anonimato, que distorsionan y protegen su identidad (Espinosa, 2019).

Según el Artículo 138° de la actual Constitución (1993), un organismo judicial es toda aquella dependencia que pertenece al Poder Judicial: Consejo Nacional de la Magistratura, el Ministerio de Justicia, la Defensoría del Pueblo, el Ministerio Público, el Tribunal Constitucional y todas aquellas dependencias que cumplen funciones vinculadas al ámbito jurisdiccional como lo es el Instituto Nacional Penitenciario, el Instituto de Medicina Legal y la Policía Nacional. El objetivo de estos organismos es el de administrar justicia (Miranda, 2007).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El tipo de investigación desarrollado en el presente trabajo es de investigación básica. Hernández et al. (2014) definió que una investigación básica es aquella que busca producir conocimiento y teorías, como es el caso de esta investigación, se busca expandir los conocimientos actuales sobre el delitos informáticos fundamentadas en teorías de otros autores que fueron influencia para la jurisprudencia de los países en los que el delitos informáticos se encuentra en una etapa más avanzada, de esta forma, los operadores de justicia podrán responder ante las amenazas de delitos informáticos pues conocerán y comprenderán la magnitud de estos delitos.

La presente investigación posee un diseño conocido como teoría fundamentada (Hernández, 2014) que define como aquella investigación que recoge e interpreta los datos, que además, supone un elemento interpretativo del significado o importancia de la problemática que se está describiendo, en tal sentido, esta investigación busca reseñar las características o rasgos de la situación problemática del objeto de estudio.

3.2. Categorías, subcategorías y matriz de categorización apriorística

Tabla 1**.**

Matriz de categorización apriorística

N°	Categoría	Subcategoría	Criterio 1	Criterio 2	Criterio 3
1	**Delitos informáticos** (Castañeda, 2015, p.37).	**Déficit normativo:** El déficit normativo puede ser interpretado como el desconocimiento de los derechos, las posibles causas	**Bien jurídico protegido** (Mayer, 2017, p. 236).	**Entorno informático (**Patiño, 2017, p. 59).	**Sujetos en el delito informático** (Posada, 2017, pp. 88-93).

		y la relación que este acto tiene sobre la efectividad en la protección del bien jurídico protegido o incluso contra la persona, esto se interpreta como el desconocimiento sobre los delitos informáticos (Arrieta et al., 2018).			
2	**Modus operandi:** Kenton (2019) explica que el modus operandi es un término en latín utilizado para describir la forma habitual de funcionamiento de un individuo o grupo, que forma un	**Perfil del delincuente informático:** Entre los perfiles de ciberdelincuentes podemos encontrar a los dependientes, los desorganizados, los desorganizados profesionalizados y los organizados. Cada uno difiere de sus técnicas	**Delitos relacionados** (Martínez, 2018, p. 7).	**Consecuencias del delito informático** (Martínez, 2018, p. 13-14).	**Operación del delito informático:** (Martínez, 2018, p. 8-9).

	patrón discernible.	y comportamiento criminal (Diago & Violat, 2020).			
3	**Intervención de órganos judiciales:** la intervención del órgano judicial comprende pues desde el inicio del juicio con la recepción del auto de apertura del delito, luego de esto, el juez debe establecer el protocolo de audiencia y la intervención está comprendida desde la investigación inicial, complementaria e intermedia (Chuquicallata, 2019).	**Eficiencia de la intervención** Especialistas de la EAE Business School (2016) definen que la eficiencia es la relación existente entre los resultados logrados y la cantidad de recursos utilizados, en tal sentido una eficiencia mayor es aquella que logra notables resultados con los mismos recursos.	**Jurisprudencia** (Cristiano & Mayorga, 2015, p. 45).	**Derecho comparado** El derecho comparado es aquella actividad que busca dimensionar los conocimientos modernos a través de la creación, investigación, proyección o práctica, por lo que, se requiere la comparación para poder captar la realidad y trabajar en ella (Sotomarino, 2019).	**Competencia judicial:** Sanromán (2016) establece que las competencias judiciales es la capacidad de actuar de manera técnica y jurídica en distintas instancias administrativas o judiciales con el debido uso de procesos, actos y procedimientos.

3.3. Escenario de estudio

Para el presente estudio de investigación se analizarán la intervención de los órganos judiciales que según Miranda (2007) son pues todas aquellas instalaciones pertenecientes al Poder Judicial y estructuradas de manera piramidal teniendo a los siguientes órganos judiciales: la corte suprema de justicia, las cortes superiores de justicia, los juzgados especializados y mixtos, los juzgados de paz letrados y los juzgados de paz.

El escenario de estudio principal para desarrollar esta investigación ha sido el uso de medios tecnológicos (laptop, celular, etc.), teniendo así la información solicitada lo mas pronto posible, pues iniciaría el dialogo con el participante en tiempo real de igual forma, todo ello sustentado pues se consignarían los correos electrónicos correspondientes, para de esta manera poder aportar conocimientos a la problemática identificada en el estudio.

3.4. Participantes

Los participantes involucrados en esta investigación son los operadores de justicia que hayan intervenido en casos de delitos informáticos, así como al ministerio público y a los abogados quienes cuentan con trayectoria en la búsqueda del delincuente informático y, se fundamentará teóricamente con fuentes de investigación provenientes de repositorios institucionales y científicos de investigación tales como Scielo y RENATI, también se contará con información de revistas especializadas en materia de legislación penal nacionales e internacionales para hallar la sustentación de la jurisprudencia en la intervención de operadores de justicia ante los delitos informáticos..

3.5. Técnicas e instrumentos de recolección de datos

Para el desarrollo de la presente investigación se utilizó la técnica de análisis documental porque según Rubio (2004) los documentos institucionales son un elemento básico para la investigación cualitativa, además de poseer un fácil acceso a una variedad de informes de investigación y artículos de revistas que mencionan el análisis de documentos como parte de la metodología.

El principal instrumento de recolección de datos para esta investigación fue la ficha de recolección de datos para la información recopilada de las revistas

indizadas y que estas a su vez puedan tener un orden específico para conocer el propósito de la investigación, el objetivo, la muestra, los resultados, la conclusión y las recomendaciones de los autores estudiados.

3.6. Procedimientos

La presente investigación recolectó la información a través de la observación estructurada, esta fue definida como Robledo (2006) como aquella que se ocupa de acopiar información para demostrar las evidencias del estudio, por lo tanto, esta investigación utilizó como instrumento principal la ficha de recolección de datos, registro anecdótico de los casos de delitos informáticos y la jurisprudencia internacional respecto a este delito. La información recopilada fue de repositorios científicos como Scielo, Dialnet, Google Académico; también de revistas online especializadas en materia jurídica utilizando palabras claves como jurisprudencia de delitos informáticos, ciberdelitos, delitos informáticos en el Perú e intervención de órganos judiciales ante los delitos informáticos.

La categorización de esta investigación se dio en función a los problemas específicos planteados agrupándolos en las categorías de normativa sobre los delitos informáticos, modus operandi e intervención de los operadores de justicia ya que la investigación gira en torno a estas variables que se interrelacionan entre sí, determinando pues sus subcategorías en el déficit normativo de los delitos informáticos, el perfil reconocido del cibercriminal y la eficiencia de la intervención.

Tabla 2.

Resumen de criterios de búsqueda

Tipo de documento	**Documentos referidos a**	**Cantidad**	**Palabras claves de búsqueda**	**Criterios de inclusión**	**Criterios de exclusión**
Artículo científico	delitos informáticos Jurisprudencia Órganos jurídicos	40	• delitos informáticos • Déficit normativo. • Intervención de la justicia.	delitos informáticos delimitado explícitamente. Jurisprudencia internacional.	delitos informáticos no especificado. Jurisprudencia inexistente.

			• Modus operandi.	Normativa internacional. Modus operandi de los delitos informáticos.	Déficit normativo. Modus operandi inexistente.
Libro	delitos informáticos	1	Modalidades de delitos informáticos.	Scaming. Grooming. Hacking. Social Engineering.	Perfiles falsos en redes sociales. Intercambio de material erótico entre parejas.
Informe técnico	-	-	-	-	-
Patente	-	-	-	-	-
Norma técnica	-	-	-	-	-
Tesis	delitos informáticos y órganos judiciales	6	Intervención de órganos judiciales delitos informáticos Modus operandi	Sentencias judiciales. Registro de cibercrímenes. Perfil del cibercriminal.	Denuncias a través de redes sociales. Capturas de pantalla sobre presuntas estafas. Testimonios no verídicos sobre delitos informáticos.

3.7. Rigor científico

Por tratarse de una investigación cualitativa se plantea una demanda de documentos críticos sobre diseño, métodos y conclusiones acerca de la intervención de los operadores de justicia ante los delitos informáticos, por lo tanto, se buscó evaluar las afirmaciones científicas de hallazgos veraces y neutrales que sean de rigor científico estricto en materia jurídica, para lo cual se presentan criterios alternativos para el rigor científico, inicialmente presentados por Lincoln y Guba: credibilidad, confiabilidad, confirmabilidad y transferibilidad (Citados por Castillo y Vásquez, 2003). Estos datos obtenidos deben ser analizados sobre la base de la teoría fundamentada.

3.8. Método de análisis de información

La presente investigación analiza la información de manera transversal logrando obtener datos de los últimos 05 años acerca de la comisión del delitos informáticos y como este ha sido castigado por los órganos judiciales en el Perú y en el mundo, por lo mismo, se estructuró tres categorías principales de investigación sobre las cuales existen bases teóricas fundamentales pues se trata de la normativa ante el delitos informáticos, el modus operandi del delitos informáticos y la intervención de los operadores de justicia ante los delitos informáticos.

Estas categorías se encuentran relacionadas entre sí ya que al no poseer una correcta normativa definiendo de manera explícita cada una de las modalidades del delitos informáticos será imposible reconocer el perfil o modus operandi de un cibercriminal en la comisión de un delito informático que a su vez convierte en limitada o nula la intervención de los operadores de justicia ante la comisión del delitos informáticos, por eso, se presentan bases teóricas que fundamentan la necesidad de contar con una normativa sólida contra el delitos informáticos.

3.9. Aspectos éticos

Según los lineamientos establecidos por el Vicerrectorado de Investigación de la Universidad César Vallejo (2020) se deben tomar en cuenta criterios que respetan y brindan garantía sobre los valores éticos en el desarrollo de la aplicación, por lo tanto, se manifiesta lo siguiente:

- El presente trabajo de investigación respeta la autoría de las fuentes de información utilizadas, citando de manera apropiada con la norma de redacción de la Asociación Americana de Psicología (APA por sus siglas en inglés).
- El presente trabajo de investigación cumple con los principios éticos del Colegio de Abogados de Lima.
- Este trabajo de investigación cumple con los aspectos fundamentales y transcendentales explicados en el código de ética de la investigación de la universidad.

IV. RESULTADOS Y DISCUSIÓN

Tabla 3:

Delitos informáticos

P1: Existen diversos bienes jurídicos que se pueden lesionar, contra el patrimonio, contra la indemnidad sexual, contra la fe pública, con la intimidad y datos de la persona. Además, estos delitos afectan al bien jurídico de la información, sea o no en una pandemia. También hay delitos por medios informáticos que afectan a la gama de bien jurídico que está establecido en el código penal. Cabe aclarar que los delitos informáticos por su propia naturaleza son pluriofensivos o multiofensivos, ya que lesionan bienes jurídicos de información privilegiada como las cuentas de bancos, tarjetas de crédito y correos electrónicos. Por último, a nivel personal podría perder la información no respaldada y su exposición sin mi consentimiento, además de un posible daño en el sistema operativo de mi computadora.

P2: Actualmente no es posible hacer frente, lo que hay no es suficiente, investigar después de, y no existe antes, “labor preventiva”. Dado que los operadores de justicia no tienen recursos para ello, Desafortunadamente el gobierno y los políticos de turno no invierten en la capacitación y recursos humanos. Como si fuera poco la normativa en materia de ciberdefensa esta, y cibercrimen también, pero digamos que hay regulación incompleta. Aún así, en el Perú no tenemos una tecnología avanzada, basta con solo ver el nivel de rapidez que tenemos en cuanto a servicio de internet, que de por si es la peor de la Región. Teniendo en cuenta que tenemos gente profesional muy capaz de poder hacerlo, pero actualmente nuestra realidad indica que existe demasiada corrupción en los cargos públicos por lo que parece que eso está muy lejano. De cualquier modo, en los medios cada vez que se reportan estos casos, no se han encontrado a los responsables de estos delitos ni tampoco se conoce el resultado final de la víctima.

P3: Intentaron realizar el fishin conmigo, sin embargo, dado mis conocimientos en esos temas no se llegó a consumar. En suma, me ha tocado ver infinidad de casos, y abogados que también pasaron por esto, debido a un chantaje de unas fotos íntimas. De manera que fui un testigo de oídas en delito informático de compras por internet, lamentablemente he visto como las víctimas en este tipo de delitos están totalmente desprotegidas, no encuentran justicia, ya que ni siquiera la propia entidad bancaria que brinda la cuenta y tarjeta afectada quiere investigar, cuando en muchas oportunidades el filtrado de información proviene desde el interior de la propia entidad bancaria. Por esta razón y por lo visto en las noticias, estas personas deben cargar con un estrés muy alto ya que el dinero perdido deben reponerlo si no fue previamente asegurado con un seguro personal o el seguro del banco en caso de tarjetas de crédito, generando un problema muy serio a nivel personal y económico.

P4: Podría ser. Pero como señale lo primordial es tener acciones preventivas por parte de las autoridades. Puesto que la capacidad en ciberseguridad es clave, empezando por los jóvenes. El adquirir un antivirus es un mecanismo, en efecto, considero que es una forma de menguar y protegerse ante posibles delitos informáticos, todo acto de prevención es útil. Aun así, me parece que no es la mejor opción ya que no estará al alcance de todos. Creo que un buen punto para empezar sería la venta de celulares clandestinos, las llamadas desde los centros penitenciarios y todo el tema de seguridad ya que estos son los que atacan o bombardean de manera más frecuente a la gente de más fácil acceso. El efecto de estos delitos tiene fuerza sobre aquellos que están desinformados sobre estas modalidades, ya que de estar informados tendrían más cuidado y sospecharían de cualquier tipo de mensaje por celular/correo/ etc. Que no parezca fiable.

Tabla 3:

Modus Operandi

P1: Por supuesto, eso pasa por que existe un desconocimiento de los políticos sobre la problemática. Es necesario su regulación pues actualmente los delincuentes adquieren esos dominios y luego de cometer sus delitos a los dos o tres días los eliminan y es difícil rastrearlos, además la información que dan los delincuentes es mayormente falsa. Desde otra perspectiva, está regulado en el TLC, capítulo de propiedad intelectual. Se encuentra dentro, solo que la gente no sabe que está ahí. Al llegar a este punto, definitivamente debe existir una regulación para su correcta aplicación y protección. En ultimas Considero que sería una buena medida para ir avanzando con la lucha contra los ataques cibernéticos, pero ante la "viveza" de los peruanos siempre hay que estar innovándose en la seguridad.

P2: Es un programa que utilizan los delincuentes para infectar la computadora a fin de pedir información. Puede agregarse que, es más frecuente de lo que se puede decir, y las compañías no lo quieren decir, y es por negligencia de ellos mismos (correo de un usuario que no debería abrir). En relación con el ransomware, pero de manera particular no conozco alguna institución que haya sido víctima de ello. Dicho de otro modo, se trata de un software que se aloja en el sistema operativo y cual parásito, toma la información personal y la copia a algún servidor en internet, donde su dueño/usuario puede tomar la decisión de permitir al virus el bloqueo de la computadora y exigir un dinero a cambio de su liberación, siendo a mi parecer un chantaje.

P3: Hay varias, pero el más común es el uso de datos del Facebook para buscar menores para pedir fotos o coaccionar a sus víctimas. También existe las compras por internet usando alguna tarjeta clonada. A primera vista dependerá mucho del sujeto afectado, si hubo más o menos impacto, pero todos son delitos, el que lo haga más grave o no, sería la pena. Sobre todo, la sustracción de información privilegiada, hurtos cibernéticos, compras por internet con tarjetas clonadas, delitos contra la libertad sexual, suplantación de identidad con la finalidad de estafar a personas ofreciendo productos de empresas que no existen, etc. Lo dicho hasta aquí supone que el phishing que es suplantar la página real con la intención de engañar al usuario y almacenar datos privados como número de tarjeta, fecha de vencimiento y cvv, y con ello proceder a realizar compras no autorizadas o simplemente cualquier tipo de transferencia, también puede ser una persona que

se hace pasar por otra con el fin de obtener tanta información como sea posible. Considero a ésta modalidad la más peligrosa pues mientras el ransomware ataca sobre todo a empresas, el phishing obtiene víctimas en todos los sectores.

Tabla 3:

Intervención de los órganos judiciales

P1: Existe pocas sentencias. En nuestro despacho fiscal se ha conseguido una condena por delito informático contra la indemnidad sexual. Como se mencionó al inicio los temas informáticos no han corrido por el poder judicial, hay casos de delitos por medios informáticos, difamación, calumnias, estafa. Sobre todo, el delito de hurto de dinero por transacciones bancarias, aquí se daría el supuesto para un delito informático al momento de la sustracción de la información de claves e información de tarjeta, sin embargo, la investigación y posterior sentencia se da bajo la norma penal del Código Penal artículo 186. En consecuencia, el poco interés y conocimiento que se tiene acerca de todo lo que involucra la vulneración de los bienes personales, se le da poca importancia. Finalmente, es posible que nuestro país no lo tome con la seriedad adecuada y se trate más de una respuesta reactiva en vez de ser preventiva. Considero que los responsables van desde el desarrollador de la aplicación web replica del original y los administradores de esa página web.

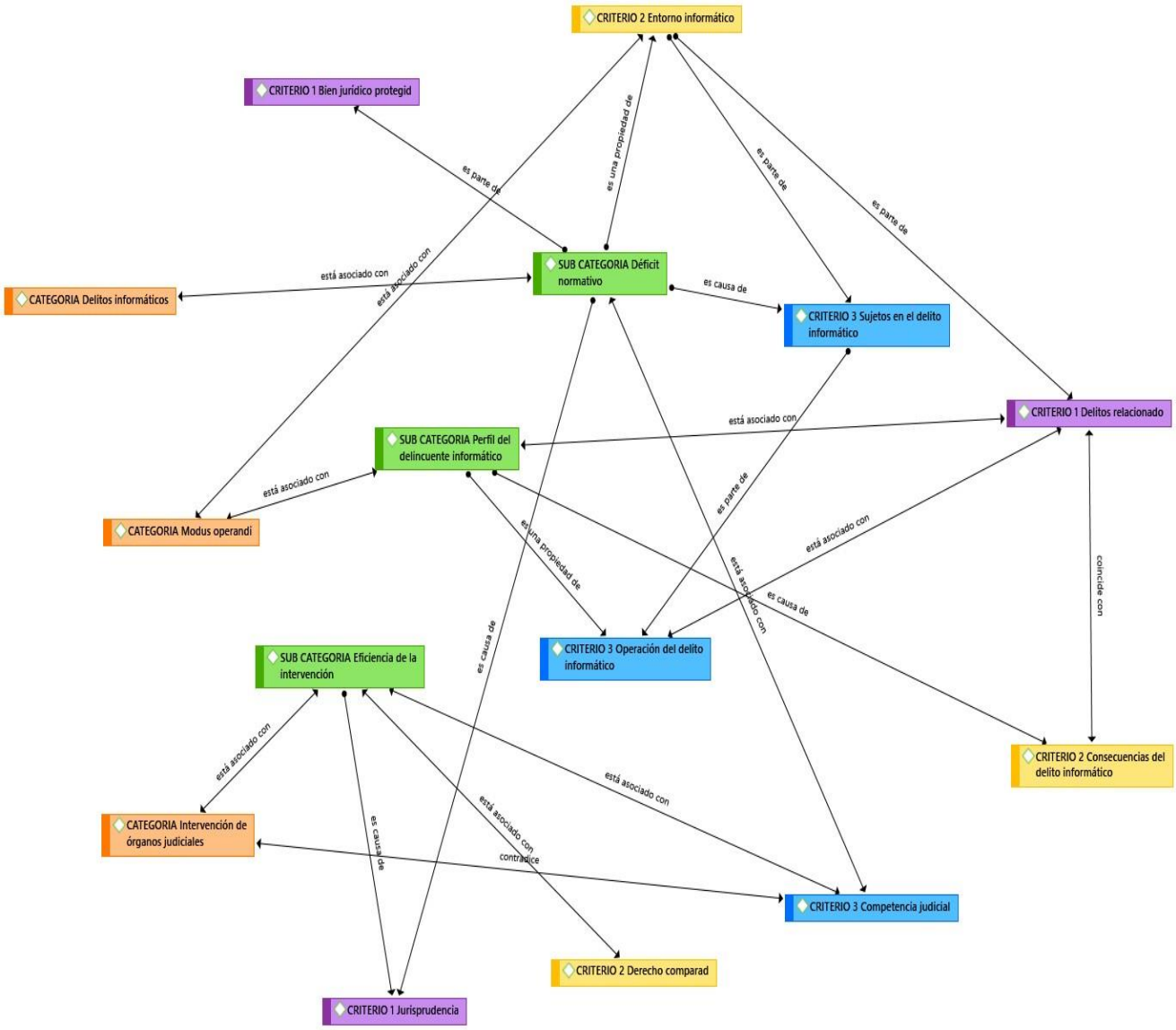
P2: Es necesaria una entidad que no solo reaccione a los hechos reportados por víctimas de estos delitos, sino también supervisión e investigación a las páginas sospechosas. Se puede incluir aquí como hay una DIVINDAD, un paralelo en la fiscalía y poder judicial. Adviértase que, a pesar de todo para investigar delitos informáticos si existe, tenemos la División de Delitos de Alta Tecnología de la PNP, es un organismo especializado para realizar investigaciones por la presunta comisión de delitos informáticos. En síntesis, sí, dado el índice de aumento de la cibercriminalidad, debe crearse juzgados y fiscalías especializadas en esos temas.

P3: Mayor personal para aligerar la carga procesal y sobre todo mayor capacitación a todos los operadores de justicia y a la PNP. En efecto sobre seguridad digital, hay cosas no conexas y no orgánicas. Políticas públicas por parte del gobierno, hasta nos hemos integrado al convenio de Budapest. También Lo principal es informar a los ciudadanos como se deben proceder ante estos casos y como poder identificarlos y también sustentarlos debidamente. Para terminar, Considero que deben supervisar el reforzamiento del nivel de seguridad de las aplicaciones web oficiales para evitar tanto como sea posible su suplantación a copias idénticas que engañen a posibles víctimas, además de brindar la opción al ciudadano de reportar páginas y/o correos sospechosos con contenido dudoso a dicha entidad para su supervisión, rastreo y posterior bloqueo.

Figura 1
Nube de palabras

Figura 2

Red de categorías, subcategorías y criterios



Este capítulo tiene como propósito, dar a conocer los resultados obtenidos, a través de la entrevista que realizamos a nuestros 5 participantes por medio del sistema ATLAS. ti. También, veremos las coincidencias, discrepancias, que se contrastaran con nuestros antecedentes y teorías ya presentadas.

Los entrevistados ELLS, EIA y CMT coinciden con el estudio que realizo Quevedo (2017) quien halló que el ciberdelito son todas las conductas sancionadas por el Código Penal y las posibles conductas aún no tipificadas. También concluye que es necesario definir al ciberdelito y distinguirlo "stricto sensu" de aquellos delitos clásicos de medio comisivo. Recomienda que cuando el ciberdelito es cometido se debe reconocer la competencia absoluta para su persecución a favor del Juez y de todos los organismos judiciales sobre los lugares donde se manifiesten los efectos del ciberdelito. Respecto a las conductas sancionadas por el código penal, en efecto estás son imputadas por el resultado obtenido, cumpliendo su propia tipificación dentro del propio cuerpo legal. Así mismo, las posibles conductas no tipificadas las encontramos en la Ley N° 30096 (Ley de Delitos informáticos), es decir con efectos punibles como la pena privativa de libertad, de modo que, teniendo en cuenta lo ya mencionado, podremos distinguirlo en *stricto sensu*, en particular de este último.

De acuerdo a lo mencionado los participantes OOC, GAZ comparan lo dicho por el autor Morrison (2020) una de las agencias de seguridad física ha informado que hay individuos que presentan como "samaritanos" y ofrecen a las personas máscaras faciales gratuitas, desinfectante para manos y otros productos cuyos suministros se han reducido durante la crisis del coronavirus. Utilizando esta técnica, los "samaritanos" están obteniendo acceso físico a los hogares de las víctimas. Con todo y lo anterior, deducimos que se refiere a la modalidad del *Phishing*, puesto que es el más común que podemos encontrar cuando entramos al navegador donde posteriormente nos dirigimos a un sitio en especial, tal como lo es *Facebook, Instagram, YouTube,* o sitios a fines preferenciales del propio usuario, esto nos lleva a páginas web donde aparecen ventanas ofreciéndote lo que usualmente sueles buscar cuando ingresas y navegas por internet. Es importante dejar claro que todo lo que realices dentro del navegador de internet o a donde te dirijas, alteraras el logaritmo propio del entorno informático, el cual en una próxima

página web que ingreses, te salen pantallas y/o anuncios ofreciéndote productos o servicios similares a los que ya, con anterioridad buscabas.

A manera de comentario, estos delitos informáticos tienen mayor fuerza a quienes desconocen del propio entrono cibernético, de sus beneficios como de sus consecuencias, aquí vale la pena decir que la constante capacitación en torno a estos delitos, se tiene que realizar de manera constante, sea dentro una entidad privada y mayormente en las públicas. Dicho de otro modo, tener agentes capaces de poder brindar un soporte y/o autoayudad en tanto estos actos de naturaleza dolosa y atípica, que es invisible ante los ojos del gobierno.

Los participantes ELLS, CMT, OOC y GAZ coinciden con Grossman (2020) que durante el mes pasado se produjo un aumento masivo en la adquisición de URL falsas, asociadas a COVID-19). Por lo general, el modus operandi es para que los scammers puedan recoger un montón de dominios relacionados con COVID-19 y convertirlos en sitios de inyección de malware malicioso. Después de que se hayan tomado todos los dominios 'buenos', los estafadores eventualmente comenzarán a aprovecharse de los dominios que contienen errores tipográficos, usando palabras como 'coronovirus' en lugar de 'coronavirus'. A primera vista, no solo se podría resumir que producto de la pandemia por coronavirus, que en efecto obligo al gobierno peruano mediante estas disposiciones aprobadas por Decreto Supremo Nº 044-2020-PCM, Nº 051-2020-PCM, N° 053-2020-PCM, Nº 094-2020-PCM, Nº 110-2020-PCM, y Nº 116-2020-PCM, por lo que se refiere a ejecutar la inmovilización social obligatoria, y focalizada en ciertos departamentos del estado peruano, con el fin de evitar la propagación, sino también que esto repercutió en la estabilidad laborad de cada uno de los ciudadanos que cuentan con contratos, a nivel privado, así mismo como a la administración pública, sus plazos procesales, de investigación preliminar, de juicio oral, lo cual significa que deberán asistir de manera remota y, de esta manera cumplir con sus funciones para lo cual fue contratado. En vista de que el desarrollo de la vida laboral se efectúa bajo esta nueva modalidad, los delincuentes comunes pasan de lado y la criminalidad de adapta al espacio cibernético, donde muy pocos conocen del tema o porque curiosidad no se informan, aprovechando este déficit para crear páginas con

nomenclatura similar a las cuales ellos ingresan, ofreciéndote productos acordes también al contexto donde se situé o las más usuales páginas web con la operatividad de efectuar pagos y/o transferencias pecuniarias a otra cuenta. Sin embargo, el interrogado EIA, manifiesta que, si se encuentras regulados en el Tratado de Libre Comercio, en el capítulo de la propiedad intelectual, y que a pesar de todo no se tiene el debido conocimiento que se requiere para reforzar nuestra propia salud cibernética.

El entrevistados EIA coincide con la teoría que presentaron Barnor y Patterson (2020) en el que señalaron que los delitos informáticos son cualquier actividad criminal que involucra un dispositivo en red o una red. Si bien la mayoría de los delitos cibernéticos se llevan a cabo con el fin de generar ganancias para los delincuentes cibernéticos, algunos delitos cibernéticos se llevan a cabo contra computadoras o dispositivos directamente para dañarlos o desactivarlos, mientras que otros usan computadoras o redes para difundir malware, información ilegal, imágenes u otros materiales. Se afirma que, los delitos son por medio comisivo, como también son el propio delito especifico, infringiendo así la Ley N° 30096, que encuentra punibilidad para estos agentes dolosos hasta con pena privativa de libertad no mayor de 6 años.

A modo de acotación, consideramos que el estudio sobre las modalidades que adoptan este tipo de delincuentes, fueron catalogadas con la denominación de *Ransonware* y el ya mencionado *Phishing*. Adviértase que, no cualquier ventana que aparezca dentro una página web de su preferencia es del todo correcta, ya que todo se encuentra en internet, pero no todo lo que se encuentra tiene es cierto.

Todos los participantes coinciden con el estudio que realizo Cajamarca (2016) donde halló que el 53% de las empresas peruanas a las que evaluaron admitieron tener poca capacidad para detectar un ataque sofisticado. Concluye que, los dispositivos no solo registran una gran cantidad de información personal. Finalmente, Cajamarca recomienda realizar un adecuado análisis forense informático requiere de un equipo multidisciplinar que incluya profesionales expertos. Es decir, que le dan validez y refuerzan el requerimiento de un equipo multidisciplinar que cumpla con las exigencias que se requieran para dicho fin, que es dar con los sujetos activos del hecho ilícito y, sancionarlos severamente con la

pena correspondiente al cuerpo legal o ley especial. Se puede incluir aquí competencias a nivel fiscalía y judicial para estos delitos que viven al margen de la adaptabilidad que nos ofrece el tiempo, la coyuntura y sobre todo la ciencia, que avanza cada día más ofreciendo un servicio transfronterizo para el que tenga acceso al internet, otorgándoles así la confianza al ciudadano de pie, que con esfuerzo y dedicación trabajan diario para obtener y trazar sus metas, así como la seguridad de un estado, de un gobierno donde también se adapte a ello y pueda alcanzar a los agresores dentro del espacio informático.

En base a la teoría los entrevistados OOC y GAZ comparan lo mencionado por Espinosa (2019) en el quien señalo que la misma manera, si existe delitos informáticos, existirán cibercriminales, los cuales son también conocidos como piratas informáticos, a menudo utilizan sistemas informáticos para obtener acceso a secretos comerciales e información personal con fines maliciosos y de explotación. Los hackers son extremadamente difíciles de identificar tanto a nivel individual como grupal debido a sus diversas medidas de seguridad, como los servidores proxy y las redes de anonimato, que distorsionan y protegen su identidad. Puesto que, en su calidad de ingenieros informáticos, aseguran que existen diversas maneras de poder realizar la clonación de páginas web, por ejemplo, las de los bancos, así como a entidades de telecomunicaciones como los la empresa Claro, Movistar, Entel, etc. Hay que mencionar que estos profesionales dan características de estos sujetos que pueden ser profesionales en diseño web, quienes crean la imagen de lo que van a supuestamente ofrecer para sustraer la información o lo que motive su accionar, esto aunado también a los propios ingenieros de sistema.

En este aspecto nosotros consideramos que debe haber una competencia especifica para estos delitos, de esta manera se lograra tener un mayor estudio y persecución del mismo, agregando a esto que el equipo interdisciplinario esta incluido a los ingenieros informáticos, técnicos en diseño web para tener una mayor dimensión del estudio de ello, esta demás decir que el aparato legal que brinda los operadores de justicia para tener una correcta persecución sin violentar otros derechos conexos ante la búsqueda del delincuente informático.

El entrevistado EIA discrepa con González (2013) quien señalaba que no hay una correcta determinación del bien jurídico protegido por los delitos de daños informáticos, recomienda que se debe crear un núcleo fácilmente reconocible en el derecho penal para así desprenderse del proceso en el cual la legislación no se ha detenido especialmente en la concepción de la ciberdelincuencia. Esto por que afirma que el bien jurídico protegido y su efecto no dependerá mucho del sujeto afectado, si no del grado del delito. A primera vista podemos entender es la gravedad del daño causado en la victima que determinara también los bienes jurídicos protegidos que han sido afectados bajo esta nueva forma, modalidad que, como ya se mencionó en los párrafos precedentes, se han ido adaptando a al contexto que nos ha tocado.

Los entrevistados ELLS, OOC Y GAZ coinciden con la teoría de Hadnagy (2018) quien señalo que el phishing es probablemente el elemento número uno que ha experimentado un aumento masivo durante estos tiempos difíciles. La sociedad tiene hambre de información, o incluso de algún tipo de alivio, y por lo tanto el phishing es mucho más exitoso durante estos tiempos. La mayoría de los ejemplos que se han visto en la naturaleza son los correos electrónicos, como las autoridades fiscales que ofrecen "reembolsos de impuestos" para ayudarlos a enfrentar la pandemia del covid-19. Todo lo que tenían que hacer era ingresar su nombre, dirección, número de teléfono, apellido de soltera de la madre y número de tarjeta bancaria, una estafa clara. Los atacantes cibernéticos también siguen muy de cerca las tendencias y noticias mundiales. Cabe concluir que, la modalidad del *Phishing* es la más exclusiva dentro de esta coyuntura, debido a su facilidad de crearse, como añadiéndole operatividad con nomenclatura similar a compra/venta de servicios o bienes, todo ello con el fin de obtener la información necesaria para hacerse con lo que haya motivado el accionar, que claramente es de aspecto pecuniario, y es más, podría asegurarse también para extorsión.

En ese aspecto consideramos que la sustracción de información privilegiada, hurtos cibernéticos, compras por internet con tarjetas clonadas, delitos contra la libertad sexual, suplantación de identidad con la finalidad de estafar a personas

ofreciendo productos de empresas que no existen, etc. Deberían de tener un castigo muy severo de índole penal, pues muchas personas se ven violentadas por medio de ese tipo de delito. Debido a que no tenemos jurisprudencia, una sentencia que confirme o revoque total o parcialmente la punibilidad del propio delito informático de manera específica, haciendo uso de las herramientas legales que tenemos dentro de nuestro ordenamiento jurídico.

V. CONCLUSIONES

Respecto a la investigación hemos llegado a las conclusiones:

1. Que los bienes jurídicos protegidos afectan en relación al daño causado por el sujeto activo, esto debido a que se tiene el desconocimiento total o parcial de la propia normativa vigente. Cabe incluir que, si bien es cierto afectan en relación al daño causado, los bienes comunes en este tipo de escenarios son la información privilegiada que contiene la victima dentro de su aparato cibernético sea este en Laptops, Celulares, Pc y Tablet, pudiendo ocasionar así un grave daño a su propio sistema operativo, secuestrando información de índole personal o a nivel nacional, dependiendo de quién sea el sujeto afectado. En cuanto hacer frente a un posible ataque masivo a nivel informático, dentro del entorno mismo, se afirma que no es suficiente con lo que tenemos, el gobierno debería invertir más en seguridad informática, por la misma razón que manejan el fondo público, como documentos de alta importancia para el estado, aquí hasta podríamos incluir secretos del mismo, como información de cada ciudadano asegurado, desde este punto mencionar a las entidades bancarias que son las que mayor tasa de reclamos se tiene por cobros fraudulentos o compras fraudulentas realizadas por no contar con un seguro incluido en tu tarjeta. Entiéndase lo antes mencionado, como una modalidad del propio delito informático denominado *Phishing*, donde ingresas a una plataforma aleatoria que te brinda servicios o productos similares a lo que posiblemente hayas requerido en su momento. Se debe agregar que hay que tener acciones preventivas que reactivas, que es a lo que el gobierno se encuentra acostumbrado.
2. Inicialmente se podría alegar que todo ello ocurre por nuestro propio descuido, esto ya mencionado al poco interés de nuestros políticos, que con la intención, quizá de obtener un control de ello, podría ser también brindar herramientas dentro del propio espacio cibernético, para así reportar o alertar de posibles paginas fraudulentas con nomenclatura similar a la obtención de datos, para así lograr realizar diversas operación en perjuicio del titular de una tarjeta de crédito, suplantando su identidad, ya que al momento de pagar no te aparece la imagen del titular para dar validez que

en si, es el titular, por si fuera poco también el pedir el documento de identidad.

3. Otro punto es, que no existen jurisprudencias y/o sentencias del propio delito informático, esto debido a que se basan en torno al resultado obtenido, como lo es por ejemplo la extorsión, mediante el secuestro de información ocasionado por el *Ransonware*, que es un *software* que ingresa a tu aparato cibernético de operatividad mediante descargas realizadas en cualquier anuncio que te rebote a la página principal y que por error hayas presionado, que secuestra información importante, exigiéndote un monto pecuniario a dicha cuenta bancaria o en *BITCOINS*, que viene a hacer la moneda digital. Por otro lado, se confirma la insistencia en crear despachos fiscales como en juzgados especializados en delitos informáticos, para un mayor estudio e interacción de estos delitos y su correcta persecución para posteriormente sea sancionado, bajo la exigencia del delito infringido, Para terminar es necesario acotar que se requiere de mayor capacitación al personal policial de la división de investigaciones de alta tecnología (DIVINDAD), así como el reforzamiento en los despachos fiscales como en los judiciales para devolver así la seguridad a las víctimas por estos delitos que han sido perjudicadas económicamente y deben manejar con el estrés de pagar lo perdido a pesar de no haber sido o haber sido inconscientemente ellos.

VI. RECOMENDACIONES

Nuestras recomendaciones para investigaciones posteriores son las siguientes:

- Creaciones de páginas web, con la operatividad de reportar a la división correspondiente de la PNP, las páginas de dudosa procedencia, así como las que hayan sido manejadas o modificadas luego de haber delinquido en otro agente y cambien su denominación adaptándose a las necesidades que surgen en aquel entonces.
- Creación de despachos fiscales como judiciales, para un mayor alcance a los delitos informáticos, obteniendo así sentencias que aporten a la identificación de estos delitos, logrando que no lleguen a consumarse y puedan encontrarse en el código penal vigente, puesto que debemos alcanzarlos dentro del entorno informático, ya que estos tiempos se están actualizando, así como la criminalidad, la tecnología, la ciencia y el derecho.
- Reforzar las medidas para combatir los delitos informáticos dentro del entorno cibernético en una nueva ley digital o utilizar, por lo menos la Ley N° 30096 (Ley de delitos informáticos), así como la revisión de directivas emanadas por las entidades estatales con relación a los servicios audiovisuales.
- Considerar que la Ley de Delitos Informáticos se encuentra vigente y operativa, hacer uso de ella para las próximas acusaciones fiscales, mediante un concurso real de delitos (Art. 50 del Código Penal), para así poder sostener bien el delito que presuntamente se le imputada.
- Por si fuera poco, el uso de la Ley ayudara a los magistrados a tener mayor consciencia y presencia la norma vigente, que si bien esta desde el año 2014, esta se vuelve dinámica y como tal, debemos avanzar junto con ello para asegurar una buen y argumentada, detallada sentencia condenatoria bajo estos delitos sofisticados.

REFERENCIAS

Alarcón, D. & Barrera, J. (2017). Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016 (Tesis de Maestría). Universidad Norbert Wiener: Lima, Perú.

Antúnez, S. (2020). Los delitos de ciberdelincuencia se disparan en confinamiento por la crisis sanitaria del Covid-19. Recuperado de: https://elderecho.com/los-delitos-ciberdelincuencia-se-disparan-confinamiento-la-crisis-sanitaria-del-covid-19

AT&T. (2020). Coronavirus Scam. Recuperado de: https://about.att.com/pages/cyberaware/ni/blog/virusscam

Barnor, J. & Patterson, A. (2020). Cybercrime Research: A Review of Research Themes, Frameworks, Methods, and Future Research Directions. Publicado en: Handbook of Research on Managing Information Systems in Developing Economies.

BBC News. (2020a). Coronavirus: US man who stockpiled hand sanitiser probed for pricegouging. Recuperado de: https://www.bbc.com/news/world-us-canada-51909045

BBC News. (2020b). Coronavirus: The fake health advice you should ignore. Recuperado de: URL: https://www.bbc.com/news/world-51735367

Beteta, J. & Narva, M. (2018). Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio (tesis de pregrado). Universidad Peruana de Ciencias Aplicadas: Lima, Perú.

Bezuidenhout, M., Mouton, F. & Venter, H. (2010). Social engineering attack detection model: SEADM. Pro-ceedings: Information Security for South Africa. Recuperado de: https://www.researchgate.net/publication/224178652_Social_engineering_attack_detection_model_SEADM

Blanco, M. (2011). Investigación narrativa: una forma de generación de conocimientos. Publicado en Argumento México, 24(67), pp. 135-156. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-57952011000300007&lng=es&tlng=es

Cajamarca, A. (2016). Implementeación de un laboratorio de informática forense en el órgano rector del Sistema de Inteligencia Nacional (Tesis de pregrado). Universidad San Ignacio de Loyola: Lima, Perú.

Castañeda, A. (2015). Complejidades y facetas del Cibercrimen. Publicado en Ciencias de la Tecnología de Información, 1(1), pp. 35-38. Recuperado de: https://www.ecorfan.org/proceedings/CTI_I/P_CTI_T_I.pdf#page=42

Castillo, E. & Vásquez, M. (2003). El rigor metodológico en la investigación cualitativa. Publicado en Colombia Médica, 34(3), pp. 164-167. Recuperado de: https://www.redalyc.org/pdf/283/28334309.pdf

Chuquicallata, F. (2019). ¿Qué es el proceso judicial? Para principiantes. Recuperado de: https://lpderecho.pe/proceso-judicial-omar-sumaria-benavente/

Contreras, A. (2003). Delitos informáticos: un importante precedente. Publicado en Ius et Praxis, 9(1), pp. 515-521. Recuperado de: https://www.researchgate.net/publication/28152505_DELITOS_INFORMATICOS_UN_IMPORTANTE_PRECEDENTE

Cristiano, K. & Mayorga, M. (2015). Análisis criminológico del cibercrimen (tesis de posgrado). Bogotá: Universidad la Gran Colombia.

De Pedro, M. (2020). Los ciberdelincuentes multiplican por 10 los dominios relacionados con el Covid-19. Recuperado de: https://directortic.es/seguridad/los-ciberdelincuentes-multiplican-por-10-los-dominios-relacionados-con-el-covid-19-2020032324183.htm

Department of Justice Delaware. (2020). Attorney General Jennings urgesconsumers to report price gouging. Recuperado de:

https://news.delaware.gov/2020/03/18/attorney-general-jennings-urges-consumers-to-report-price- gouging/

Diago, L. & Violat, M. (2020). El perfil del ciberdelincuente: los patrones del mal. Recuperado de: https://derechodelared.com/perfil-ciberdelincuente/

Espinosa, J. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. Publicado en: La Razón histórica: revista hispanoamericana de historia de las ideas políticas y sociales, 44, pp. 153-173.

Ferre-Sadurni, L. & McKinley, J. (2020). Alex Jones Is Told to Stop SellingSham Anti-Coronavirus Toothpaste. Recuperado de: https://www.nytimes.com/2020/03/13/nyregion/alex-jones-coronavirus-cure.html

Fowler, H. & Duncan, C. (2020). Hackers made their own coronavirus map to spread mal-ware, feds warn. Recuperado de: https://www.miamiherald.com/news/nation-world/national/article241171546.html

Gobierno del Perú. (2004). Decreto Legislativo N°957 Código Procesal Penal. Obtenido de: http://www.oas.org/juridico/PDFs/mesicic5_per_3_dec_leg_957.pdf

Gómez, A. (2020). Cómo está afectando la expansión del COVID-19 a la ciberdelincuencia. Recuperado de: https://www.bbva.com/es/como-esta-afectando-la-expansion-del-covid-19-a-la-ciberdelincuencia/

González, J. (2013). Delincuencia informática: Daños informáticos del Artículo 264 del Código Penal y propuesta de reforma (tesis doctoral). Universidad Complutense de Madrid: Madrid, España.

Grossman, J. (2020). Corono .com domains registered. Recuperado de: https://twitter.com/jeremiahg/status/1234612630880321537

Hadnagy, C. (2018). Social Engineering The Science of Human Hacking. Wiley: Toronto.

Herman, P. & Henry, K. (2020). Coronavirus lies — Debunking the hoaxes around Covid-19. Recuperado de:

https://www.news24.com/SouthAfrica/News/dettol-garlic-and-fake- cases-in-north- west-cape-debunking- the-hoaxes-lies-around-coronavirus-20200306

Hernández, R., Collado, C. & Baptista, M. (2014). Metodología de la Investigación. McGraw-Hill: México D.F.

Larios, J. & Sánchez, R. (2014). Ciberdelito (tesis de pregrado). Univerisdad Nacional Autónoma de México: México D.F., México.

Ley N°30170. (2014). Ley de Delitos Informáticos. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/200326/197055_Ley30171.pdf20180926-32492-1l0lzim.pdf

Martínez, L. (2018). El cibercrimen en Colombia (Ensayo). Universidad Militar Nueva Granada: Bogotá.

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista chilena de derecho, 44(1), pp. 235-260. Recuperado de: https://dx.doi.org/10.4067/S0718-34372017000100011

Miranda, M. (2007). Estructura organizacional piramidal de los órganos jurisdiccionales en el Perú y en el extranjero. Publicado en Revista Oficial del Poder Judicial 1(1), pp. 85-106. Recuperado de: https://www.pj.gob.pe/wps/wcm/connect/133b090043eb7b7aa6a9e74684c6236a/5+Doctrina+Nacional+-+Magistrados+-+Miranda+Canales.pdf?MOD=AJPERES&CACHEID=133b090043eb7b7aa6a9e74684c6236a

Miranda, M. (2007). Estructura organizacional piramidal de los órganos jurisdiccionales en el Perú y en el extranjero. Publicado en Revista Oficial del Poder Judicial, 1(1), pp. 85-106.

Morrison, S. (2020). Coronavirus email scams are trying to cash in on your fear. Recuperado de: https://www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams

Mouton, F., Leenen, L., Malan, M. & Venter, H. (2014). Towards an Ontological Model Defining the Social Engineering Domain. Recuperado de:

https://www.researchgate.net/publication/263588276_Towards_an_Ontological_Model_Defining_the_Social_Engineering_Domain

Nelson, D. (2020). Thieves Swindle $2M From Coronavirus Preppers WithHand Sanitizer, Face Mask Scams. Recuperado de: https://www.coindesk.com/thieves-swindle-2m-from-coronavirus-preppers-with-hand-sanitizer-face-mask-scam

Patiño, R. (2017). Afectación del cibercrimen en las pymes. Publicado en Memorias: Segundo Congreso Internacional: Crimen económico y fraude financiero y contable. Recuperado de: https://www.researchgate.net/profile/Ludivia_Aros/publication/320339411_El_capital_humano_en_el_desarrollo_del_encargo_de_auditoria_acercamiento_desde_las_Normas_Internacionales_de_Control_de_Calidad/links/5b1591a90f7e9bda0ffdf74a/El-capital-humano-en-el-desarrollo-del-encargo-de-auditoria-acercamiento-desde-las-Normas-Internacionales-de-Control-de-Calidad.pdf#page=59

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Publicado en: Nuevo Foro Penal, 1(88), pp. 72-112.

Quevedo, J. (2017). Investigación y prueba del ciberdelito (tesis de doctorado). Universitat de Barcelona: Barcelona, España.

Robledo, C. (2006). Técnicas y proceso de investigación. Universidad de San Carlos de Guatemala. Recuperado de: https://investigar1.files.wordpress.com/2010/05/fichas-de-trabajo.pdf

Rubio, M. (2004). El análisis documental : indización y resumen en bases de datos especializadas. Recuperado de: http://eprints.rclis.org/6015/1/An%C3%A1lisis_documental_indizaci%C3%B3n_y_resumen.pdf

Sotomarino, R. (2019). La importancia del Derecho Comparado a partir de la comprensión de los estilos jurídicos. Publicado en Polémos. Recuperado de: https://polemos.pe/la-importancia-del-derecho-comparado-partir-la-comprension-los-estilos-juridicos/

Tarun, R. (2020). COVID-19 Social Engineering Attacks. Recuperado de: https://www.csoonline.com/article/3533339/covid-19-social-engineering-attacks.html

ANEXOS

FORMULARIO DE CONSENTIMIENTO INFORMADO

El ENTREVISTADO Gustavo Alfonso Arrelucea Zapata natural de Lima - Perú con domicilio en Calle Mitobamba 5076 – Urb. Parque el Naranjal Localidad Los Olivos Provincia Lima con edad de 27 años y DNI 71311987, y abajo firmante, ha sido INFORMADO DETALLADAMENTE SOBRE EL ESTUDIO "**Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19"** que de forma resumida:

Nuestra investigación propone brindar un concepto diferente a los operadores de justicia, haciendo valer la ley 30096 (Ley de delitos informáticos), donde no sea únicamente el objeto (laptop, celular, iPad, pc's, etc.) el medio para llegar a cierto fin, encontrándose la punibilidad dentro del cogido penal (extorsión, estafa, etc.), sino donde podamos alcanzar al sujeto activo dentro del sistema informático, sancionarlo o en sus efectos de la misma ley ya mencionada, aplicar penas limitativas de derecho y de esta manera reforzar la seguridad a la información, que día a día avanza a un paso silencioso.

Se le ha informado sobre los alcances hallados y los objetivos trazados en el presente estudio, siendo los principales problemas los siguientes:

- Existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por COVID-19.
- Existe un déficit normativo en la ley de delitos informáticos que debilita la intervención de los operadores de justicia.
- Hay un perfil para el reconocimiento por parte de los operadores de justicia del modus operandi en la comisión del delito informático.
- Existía intervención de los operadores de justicia a las amenazas de delitos informáticos antes del estado de emergencia por COVID-19.

Asimismo, se le ha informado de que:

- sus datos se tratarán de forma confidencial;
- su participación en el estudio es voluntaria;
- su consentimiento para participar puede ser retirado en cualquier momento, sin que esta decisión perjudique el trato que reciba por los sustentantes.

He tenido la oportunidad de preguntar sobre mi participación en el estudio y se me ha contestado satisfactoriamente las preguntas que he realizado.

En la fecha, 09 de septiembre del año 2020

SUSTENTANTES

Andy Antonio Ortiz Cahuana

Martin Leopol Adarmes Alvarez

EL ENTREVISTADO

Gustavo Alfonso Arrelucea Zapata

FORMULARIO DE CONSENTIMIENTO INFORMADO

EL ENTREVISTADO Carlos MEZA Trujillo Natural de Lima con domicilio en STA ELVIRA M2C. Localidad los olivos Provincia Lima con edad de 38 años y DNI 41[illegible] abajo firmante, ha sido INFORMADO DETALLADAMENTE SOBRE EL ESTUDIO "**Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19"** que de forma resumida:

Nuestra investigación propone brindar un concepto diferente a los operadores de justicia, haciendo valer la ley 30096 (Ley de delitos informaticos), donde no sea unicamente el objeto (laptop, celular, ipad, pc's, etc.) el medio para llegar a cierto fin, encontrandose la punibilidad dentro del cogido penal (extorsión, estafa, etc.), sino donde podamos alcanzar al sujeto activo dentro del sistema informatico, sancionarlo o en sus efectos de la misma ley ya mencionada, aplicar penas limitativas de derecho y de esta manera reforzar la seguridad a la información, que día a día avanza a un paso silencioso.

Se le ha informado sobre los alcances hallados y los objetivos trazados en el presente estudio, siendo los principales problemas los siguientes:

- Existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informaticos durante el estado de emergencia por COVID-19.
- Existe un deficit normativo en la ley de delitos informaticos que debilita la intervencion de los operadores de justicia.
- Hay un perfil para el reconomiento por parte de los operadores de justicia del modus operandi en la comisión del delito informatico.
- Existia intervención de los operadores de justicia a las amenazas de delitos informaticos antes del estado de emergencia por COVID-19.

Asimismo, se le ha informado de que:

- sus datos se tratarán de forma confidencial;
- su participación en el estudio es voluntaria;
- su consentimiento a participar puede ser retirado en cualquier momento, sin que esta decisión perjudique el trato que reciba por los sustentantes.

He tenido la oportunidad de preguntar sobre mi participación en el estudio y se me ha contestado satisfactoriamente las preguntas que he realizado.

En la fecha, 09 de septiembre del año 2020

SUSTENTANTES

Andy Antonio Ortiz Cahuana
71080243
Martin Leopol Adarmes Alvarez
74831457

EL ENTREVISTADO

Carlos MEZA Trujillo

FORMULARIO DE CONSENTIMIENTO INFORMADO

El ENTREVISTADO erick iriarte ahon natural de lima con domicilio en lima Localidad lima y DNI 10803692 y abajo firmante, ha sido INFORMADO DETALLADAMENTE SOBRE EL ESTUDIO "**Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19"** que de forma resumida:

Nuestra investigación propone brindar un concepto diferente a los operadores de justicia, haciendo valer la ley 30096 (Ley de delitos informaticos), donde no sea unicamente el objeto (laptop, celular, ipad, pc's, etc.) el medio para llegar a cierto fin, encontrandose la punibilidad dentro del cogido penal (extorsión, estafa, etc.), sino donde podamos alcanzar al sujeto activo dentro del sistema informatico, sancionarlo o en sus efectos de la misma ley ya mencionada, aplicar penas limitativas de derecho y de esta manera reforzar la seguridad a la información, que dia a dia avanza a un paso silencioso.

Se le ha informado sobre los alcances hallados y los objetivos trazados en el presente estudio, siendo los principales problemas los siguientes:

- Existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informaticos durante el estado de emergencia por COVID-19.
- Existe un deficit normativo en la ley de delitos informaticos que debilita la intervencion de los operadores de justicia.
- Hay un perfil para el reconomiento por parte de los operadores de justicia del modus operandi en la comisión del delito informatico.
- Existia intervención de los operadores de justicia a las amenazas de delitos informaticos antes del estado de emergencia por COVID-19.

Asimismo, se le ha informado de que:

- sus datos se tratarán de forma confidencial;
- su participación en el estudio es voluntaria;
- su consentimiento a participar puede ser retirado en cualquier momento, sin que esta decisión perjudique el trato que reciba por los sustentantes.

He tenido la oportunidad de preguntar sobre mi participación en el estudio y se me ha contestado satisfactoriamente las preguntas que he realizado.

En la fecha, 09 de septiembre del año 2020

SUSTENTANTES

Andy Antonio Ortiz Cahuana

Martin Leopol Adarmes Alvarez

EL ENTREVISTADO

FORMULARIO DE CONSENTIMIENTO INFORMADO

El ENTREVISTADO Oscar Adrian Ortiz Cahuana natural de Perú con domicilio en Jr. Corrientes 207 AAHH Villa Hermoza Localidad El Agustino Provincia Lima con edad de 28 años y DNI 71080242, y abajo firmante, ha sido INFORMADO DETALLADAMENTE SOBRE EL ESTUDIO "**Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19"** que de forma resumida:

Nuestra investigación propone brindar un concepto diferente a los operadores de justicia, haciendo valer la ley 30096 (Ley de delitos informáticos), donde no sea únicamente el objeto (laptop, celular, ipad, pc's, etc.) el medio para llegar a cierto fin, encontrándose la punibilidad dentro del cogido penal (extorsión, estafa, etc.), sino donde podamos alcanzar al sujeto activo dentro del sistema informático, sancionarlo o en sus efectos de la misma ley ya mencionada, aplicar penas limitativas de derecho y de esta manera reforzar la seguridad a la información, que día a día avanza a un paso silencioso.

Se le ha informado sobre los alcances hallados y los objetivos trazados en el presente estudio, siendo los principales problemas los siguientes:

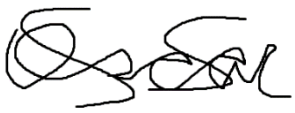
- Existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por COVID-19.
- Existe un déficit normativo en la ley de delitos informáticos que debilita la intervención de los operadores de justicia.
- Hay un perfil para el reconomiento por parte de los operadores de justicia del modus operandi en la comisión del delito informático.
- Existía intervención de los operadores de justicia a las amenazas de delitos informáticos antes del estado de emergencia por COVID-19.

Asimismo, se le ha informado de que:

- sus datos se tratarán de forma confidencial;
- su participación en el estudio es voluntaria;
- su consentimiento a participar puede ser retirado en cualquier momento, sin que esta decisión perjudique el trato que reciba por los sustentantes.

He tenido la oportunidad de preguntar sobre mi participación en el estudio y se me ha contestado satisfactoriamente las preguntas que he realizado.

En la fecha, 09 de septiembre del año 2020



SUSTENTANTES

Andy Antonio Ortiz Cahuana

Martin Leopol Adarmes Alvarez

EL ENTREVISTADO

FORMULARIO DE CONSENTIMIENTO INFORMADO

El ENTREVISTADO **ENRIQUE VICTOR LLONTOP SILVA** natural de LIMA con domicilio en Jirón Los Líquenes 550, urbanización Las Flores, San Juan de Lurigancho Provincia de Lima con edad de 36 años y DNI N° 42160828, y abajo firmante, ha sido INFORMADO DETALLADAMENTE SOBRE EL ESTUDIO "**Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19"** que de forma resumida:

Nuestra investigación propone brindar un concepto diferente a los operadores de justicia, haciendo valer la ley 30096 (Ley de delitos informáticos), donde no sea únicamente el objeto (laptop, celular, ipad, pc's, etc.) el medio para llegar a cierto fin, encontrándose la punibilidad dentro del cogido penal (extorsión, estafa, etc.), sino donde podamos alcanzar al sujeto activo dentro del sistema informático, sancionarlo o en sus efectos de la misma ley ya mencionada, aplicar penas limitativas de derecho y de esta manera reforzar la seguridad a la información, que día a día avanza a un paso silencioso.

Se le ha informado sobre los alcances hallados y los objetivos trazados en el presente estudio, siendo los principales problemas los siguientes:

- Existe intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por COVID-19.
- Existe un déficit normativo en la ley de delitos informáticos que debilita la intervención de los operadores de justicia.
- Hay un perfil para el reconocimiento por parte de los operadores de justicia del modus operandi en la comisión del delito informático.
- Existía intervención de los operadores de justicia a las amenazas de delitos informáticos antes del estado de emergencia por COVID-19.

Asimismo, se le ha informado de que:

- Sus datos se tratarán de forma confidencial;
- Su participación en el estudio es voluntaria;
- Su consentimiento a participar puede ser retirado en cualquier momento, sin que esta decisión perjudique el trato que reciba por los sustentantes.

He tenido la oportunidad de preguntar sobre mi participación en el estudio y se me ha contestado satisfactoriamente las preguntas que he realizado.

En la fecha, 09 de septiembre del año 2020

SUSTENTANTES

Andy Antonio Ortiz Cahuana

Martin Leopol Adarmes Alvarez

EL ENTREVISTADO

ENRIQUE VICTOR LLONTOP SILVA

DNI N° 42160828

Anexo 3: Ficha De Entrevista

Dirigido a especialistas en el ámbito de Derecho Penal

Título: Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19

Nombre del entrevistado: GUSTAVO ALFONSO ARRELUCEA ZAPATA

Edad: 27 años

Sexo: MASCULINO

Ocupación: ANALISTA DE SOLUCIONES BI

Fecha de la entrevista: 15/09/2020

Entrevistador: Andy Antonio Ortiz Cahuana – Martin Leopol Adarmes Alvarez

Entrevistarlo respecto:

1.- ¿Teniendo en cuenta la coyuntura en la cual nos encontramos, que bienes jurídicos protegidos son vulnerados por los delitos informáticos?

Las cuentas de bancos, tarjetas de crédito y correos electrónicos.

2.- Según su experiencia ¿Desde la creación de la ley 27309 (Ley de delitos informáticos) y su derogación por la ley 30096 siendo modificada por la ley 30171, a la fecha no se ha visto una sentencia judicial que hable con respecto a estos delitos informáticos, a que cree que se deba esto?

El poco interés y conocimiento que se tiene acerca de todo lo que involucra la vulneración de los bienes personales, se le da poca importancia a esto ya que aún son pocos casos y la mayoría no son denunciados por el poco foco que se le da y además de lo difícil que para algunos es demostrar que de verdad hubo un delito.

3.- Se entiende por competencia judicial a todo ente encargado de actuar de manera técnica y jurídica en distintas instancias, conociendo la complejidad de estos delitos informáticos ¿cree usted que sea necesario crear una competencia judicial específica para el mejor entendimiento de estos delitos informáticos?

Creo que si, ya que, si bien aún son pocos estos casos, es bueno darle foco desde el inicio para que cuando se presenten nuevos acontecimientos se sepa que hacer y como proceder para salvaguardar nuestros bienes.

4.- ¿Qué acciones considera usted que se deba optar por nuestros órganos de justicia para hacer frente a los delitos informáticos?

Lo principal es informar a los ciudadanos como se deben proceder ante estos casos y como poder identificarlos y también sustentarlos debidamente.

5. ¿Considera Ud. que el Perú se encuentra en la capacidad jurídica de poder hacer frente a un ataque cibernético a entidades públicas y privadas?

Creo que tenemos gente profesional muy capaz de poder hacerlo, pero actualmente nuestra realidad indica que existe demasiado corrupción en los cargos públicos por lo que parece que eso está muy lejano.

6. ¿Considera Ud. Que el hosting de aplicaciones y la venta/uso de dominios con nomenclatura similar a marcas existentes deba ser regulado?

Considero que sería una buena medida para ir avanzando con la lucha contra los ataques cibernéticos, pero ante la "viveza" de los peruanos siempre hay que estar innovándose en la seguridad.

7. ¿Fue Ud. Testigo o víctima de la ciberdelincuencia? Sí fue así, cuál ha sido la consecuencia mental/laboral/personal en dicha persona luego de ser víctima de esta modalidad de delincuencia, sea compras no autorizadas por internet, retiro de dinero en nombre suyo sin consentimiento, etc?

Felizmente hasta ahora no he sido victima de ello.

8. ¿Conoce Ud. sobre el RansomWare? De ser así, sin mencionar el nombre de la Institución, ¿fue su institución o alguna otra que Ud. conozca víctima de ello?

Si conozco sobre el RansomWare, pero de manera particular no conozco aguna institución que haya sido victima de ello.

9. ¿Opina Ud. Que la solución para evitar ser víctima sea adquirir antivirus más potentes a nivel personal/empresarial? En caso de que considere que no lo es, ¿podría sugerir una solución?

Me parece que no es la mejor opción ya que no estará al alcance de todos. Creo que un buen punto para empezar sería la venta de celulares clandestinos, las llamadas desde los centros penitenciarios y todo el tema de seguridad ya que estos son los que atacan o bombardean de manera más frecuente a la gente de más fácil acceso.

10. ¿Podría Ud. Listar las modalidades de ciberdelincuencia más comunes, así como también conocer su opinión sobre la cual Ud. Considere mas peligrosa y/o común?

- **Envío de mensajes de texto sobre información de cuentas bancarias.**
- **Envío de correos electrónicos con links para el robo de información.**
- **Páginas web con dominio similar a las de las entidades bancarias.**

A mi parecer la más común y por ende más peligrosa por estar al alcance de cada uno y de la rutina diaria es el envío de mensajes de texto ya que hoy en día la gran mayoría cuenta con un celular y al ver esto puede asustarse y pensar lo peor en el momento por lo cual accede a abrir links y seguir las indicaciones que contiene este mensaje.

Anexo 3: Ficha De Entrevista

Dirigido a especialistas en el ámbito de Derecho Penal e Informatica

Título: Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19

Nombre del entrevistado:

Edad:

Sexo:

Ocupación:

Fecha de la entrevista:

Entrevistador: Andy Antonio Ortiz Cahuana – Martin Leopol Adarmes Alvarez

Entrevistarlo respecto:

1.- ¿Teniendo en cuenta la coyuntura en la cual nos encontramos, que bienes jurídicos protegidos son vulnerados por los delitos informáticos?

Existen diversos bienes juridicos que se pueden leisonar, contra el patrimonio, con la indemnidad sexual, contra la fe publica, con la intimidad y datos de la persona.

2.- Según su experiencia ¿Desde la creación de la ley 27309 (Ley de delitos informáticos) y su derogación por la ley 30096 siendo modificada por la ley 30171, a la fecha no se ha visto una sentencia judicial que hable con respecto a estos delitos informáticos, a que cree que se deba esto?

Existe pocas sentencias. En nuestro despacho fiscal se ha conseguido una condena por delito informatico contra la indemnidad sexual.

3.- Se entiende por competencia judicial a todo ente encargado de actuar de manera técnica y jurídica en distintas instancias, conociendo la complejidad de

estos delitos informáticos ¿cree usted que sea necesario crear una competencia judicial específica para el mejor entendimiento de estos delitos informáticos?

Por supuesto que si, dado el indice de aumento de la cibercriminalidad, debe crearse juzgados y fiscalias especializadas en esos temas.

4.- ¿Qué acciones considera usted que se deba optar por nuestros órganos de justicia para hacer frente a los delitos informáticos?

Mayor personal para aligerar la carga procesal y sobre todo mayor capacitación a todos los operadores de justicia a la PNP.

5. ¿Considera Ud. que el Perú se encuentra en la capacidad jurídica de poder hacer frente a un ataque cibernético a entidades públicas y privadas?

Actualmente no es posible hacer frente, lo que hay no es suficient, investigar despues de, y no existe antes, “labor preventiva”. Ello, dado que los operados de justicia no tienen recursos para ello, Desgraciadamente el gobierno y los politicos de turno no invierten en la capacitación y recursos humanos.

6. ¿Considera Ud. Que el hosting de aplicaciones y la venta/uso de dominios con nomenclatura similar a marcas existentes deba ser regulado?

Por supuesto, eso pasa por que existe un desconocimiento de los politicos sobre la problematicas. Es necesario su regulación pues actualmente los delincuentes adquieren esos dominios y luego de cometer sus delitos a los dos o tre dias los eliminan y es dificil rastrearlos, ademas la información que dan los delincuentaes son mayormente falsos.

7. ¿Fue Ud. Testigo o víctima de la ciberdelincuencia? Sí fue así, cuál ha sido la consecuencia mental/laboral/personal en dicha persona luego de ser víctima de esta modalidad de delincuencia, sea compras no autorizadas por internet, retiro de dinero en nombre suyo sin consentimiento, etc?

Intentaron realizar el fishin conmigo sin embargo, dada mis conocimientos en esos temas no se llego a consumar.

8. ¿Conoce Ud. sobre el RansomWare? De ser así, sin mencionar el nombre de la Institución, fue su Institución o alguna otra que Ud. Conozca víctima de ello?

Es un programa que utilizan los delincuentes para infectar la computadora a fun de pedir información.

9. ¿Opina Ud. Que la solución para evitar ser víctima sea adquirir antivirus más potentes a nivel personal/empresarial? En caso de que considere que no lo es, podría sugerir una solución?

Podria ser. Pero como señale la primordial es tener acciones preventivas por parte de las autoridades.

10. ¿Podría Ud. Listar las modalidades de ciberdelincuencia más comunes, así como también conocer su opinión sobre la cual Ud. Considere mas peligrosa y/o común?

Hay varias, pero el mas comun es el uso de datos del facebook para buscar menores para pedir fotos o coaccionar a sus victimas, tamgien el fishi en cual piden claves por celular creando una plataforma falsa de alguna empresa como Claro o algun banco. Tambien existe las compras por internet usando alguna tarjeta clonada.

Anexo 3: Ficha De Entrevista

Dirigido a especialistas en el ámbito de Derecho Penal e Informatica

Título: Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19

Nombre del entrevistado:

Edad:

Sexo:

Ocupación:

Fecha de la entrevista:

Entrevistador: Andy Antonio Ortiz Cahuana – Martin Leopol Adarmes Alvarez

Entrevistarlo respecto:

1.- ¿Teniendo en cuenta la coyuntura en la cual nos encontramos, que bienes jurídicos protegidos son vulnerados por los delitos informáticos?

La conyuntura no tiene nada que ver, estos delitos afectan al bien juridico información, sea o no en una pandemia. También hay delitos por medios informaticos que afectan a la gama de bien juridico que esta establecido en el codigo penal.

2.- Según su experiencia ¿Desde la creación de la ley 27309 (Ley de delitos informáticos) y su derogación por la ley 30096 siendo modificada por la ley 30171, a la fecha no se ha visto una sentencia judicial que hable con respecto a estos delitos informáticos, a que cree que se deba esto?

Fundmentalmente en general los temas informaticos no han corrido por el poder judicial, hay casos de delitos por medios informaticos difamacion calumnias estafa, el caso mas renombrado de un delito de apariencia electronica de fondos CROWEL

PALACIOS, gerente del BBVA y no quiere la SBS que nadie lo sepa, por un tema de imagen, lo resuelven de una manera interna.

3.- Se entiende por competencia judicial a todo ente encargado de actuar de manera técnica y jurídica en distintas instancias, conociendo la complejidad de estos delitos informáticos ¿cree usted que sea necesario crear una competencia judicial específica para el mejor entendimiento de estos delitos informáticos?

Tiene que ver tanto una fiscalia especializada en delitos informaticos, como un juzgado especialista en temas digitales. Asi como hay una DIVINDAD, un paralelo en la fiscalia y poder judicial.

4.- ¿Qué acciones considera usted que se deba optar por nuestros órganos de justicia para hacer frente a los delitos informáticos?

Se ha desarrollado capacidad en jueces y fiscales en la AMAG, la fiscalia avanzo en manuales de informatica forense, ahy temas ligados en DU 007, sobre seguridad digital, hay cosas no conexas y no organicas. Politicas publicas por parte del gobierno, hasta nos hemos integrado al convenio de Budapest.

5. ¿Considera Ud. que el Perú se encuentra en la capacidad jurídica de poder hacer frente a un ataque cibernético a entidades públicas y privadas?

La normativa en materia de ciberdefensa esta, y cibercrimen tambien, pero digamos que hay regulacion incompleta.

6. ¿Considera Ud. Que el hosting de aplicaciones y la venta/uso de dominios con nomenclatura similar a marcas existentes deba ser regulado?

Esta regulado en el TLC, capitulo de propiedad intelectual. Se encuentra dentro, solo que la gente no sabe que esta ahi.

7. ¿Fue Ud. Testigo o víctima de la ciberdelincuencia? Sí fue así, cuál ha sido la consecuencia mental/laboral/personal en dicha persona luego de ser víctima de esta modalidad de delincuencia, sea compras no autorizadas por internet, retiro de dinero en nombre suyo sin consentimiento, etc?

Me ha tocado ver infinidad de casos, y abogados que tambien pasaron por esto, debido a un chantaje de unas fotos intimas y perdio su matromonio.

8. ¿Conoce Ud. sobre el RansomWare? De ser así, sin mencionar el nombre de la Institución, fue su Institución o alguna otra que Ud. Conozca víctima de ello?

Si, es mas frecuente de lo que se puede decir, y las compañias no lo quieren decir, y es por neglicencia de ellos mismos (correo de un usuario que no deberia abrir).

9. ¿Opina Ud. Que la solución para evitar ser víctima sea adquirir antivirus más potentes a nivel personal/empresarial? En caso de que considere que no lo es, podría sugerir una solución?

La solucion es, muchos pueden entrar a paginas, u correos que no deberian abrir, entonces la capacidad en ciberseguridad es clave, empezando por los jovenes. El adquirir un antivirus es un mecanismo, pero así como hay medicamentos, que salen cuando hay enfermedades emergentes sale.

10. ¿Podría Ud. Listar las modalidades de ciberdelincuencia más comunes, así como también conocer su opinión sobre la cual Ud. Considere mas peligrosa y/o común?

Dependera mucho del sujeto afectado, si hubo mas o menos impacto, pero todos son delitos, el que lo haga mas grave o no, sería la pena.

Anexo 3: Ficha De Entrevista

Dirigido a especialistas en el ámbito de Derecho Penal

Título: Intervención de los operadores de justicia ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19

Nombre del entrevistado: Oscar Adrián Ortiz Cahuana

Edad: 27

Sexo: Masculino

Ocupación: Software Engineer

Fecha de la entrevista: 16/09/2020

Entrevistador: Andy Antonio Ortiz Cahuana – Martin Leopol Adarmes Alvarez

Entrevistarlo respecto:

1.- ¿Teniendo en cuenta la coyuntura en la cual nos encontramos, que bienes jurídicos protegidos son vulnerados por los delitos informáticos?

Entendería información confidencial y personal de la Empresa si hablamos a nivel de que el delito fuese a una red privada/externa de una empresa, a nivel personal podría perder la información no respaldada y su exposición sin mi consentimiento, además de un posible daño en el sistema operativo de mi computadora.

2.- Según su experiencia ¿Desde la creación de la ley 27309 (Ley de delitos informáticos) y su derogación por la ley 30096 siendo modificada por la ley 30171, a la fecha no se ha visto una sentencia judicial que hable con respecto a estos delitos informáticos, a que cree que se deba esto?

Es posible que nuestro país no lo tome con la seriedad adecuada y se trate más de una respuesta reactiva en vez de ser preventiva. Considero que los

responsables van desde el desarrollador de la aplicación web replica del original y los administradores de esa página web.

3.- Se entiende por competencia judicial a todo ente encargado de actuar de manera técnica y jurídica en distintas instancias, conociendo la complejidad de estos delitos informáticos ¿cree usted que sea necesario crear una competencia judicial específica para el mejor entendimiento de estos delitos informáticos?

Sí, es necesaria una entidad que no solo reaccione a los hechos reportados por víctimas de estos delitos, sino también supervisión e investigación a las páginas sospechosas.

4.- ¿Qué acciones considera usted que se deba optar por nuestros órganos de justicia para hacer frente a los delitos informáticos?

Considero que deben supervisar el reforzamiento del nivel de seguridad de las aplicaciones web oficiales para evitar tanto como sea posible su suplantación a copias idénticas que engañen a posibles víctimas, además de brindar la opción al ciudadano de reportar paginas y/o correos sospechosos con contenido dudoso a dicha entidad para su supervisión, rastreo y posterior bloqueo.

5. ¿Considera Ud. que el Perú se encuentra en la capacidad jurídica de poder hacer frente a un ataque cibernético a entidades públicas y privadas?

No, por lo visto en los medios cada vez que se reportan estos casos no hay ni una sola noticia que indique se han encontrado a los responsables de estos delitos ni tampoco se conoce el resultado final de la víctima frente a los bancos, por lo que creo que simplemente se deja de lado el caso y se archiva como cualquier otro caso sin consecuencia legal.

6. ¿Considera Ud. Que el hosting de aplicaciones y la venta/uso de dominios con nomenclatura similar a marcas existentes deba ser regulado?

Sí, reduciría significativamente las direcciones web con nombre similar y evitar confusión a los usuarios comunes.

7. ¿Fue Ud. Testigo o víctima de la ciberdelincuencia? Sí fue así, cuál ha sido la consecuencia mental/laboral/personal en dicha persona luego de ser víctima de

esta modalidad de delincuencia, sea compras no autorizadas por internet, retiro de dinero en nombre suyo sin consentimiento, etc?

No he sido víctima ni tengo un contacto cercano víctima de ello, pero por lo visto en las noticias, estas personas deben cargar con un estrés muy alto ya que el dinero perdido deben reponerlo si no fue previamente asegurado con un seguro personal o el seguro del banco en caso de tarjetas de crédito, generando un problema muy serio a nivel personal y económico.

8. ¿Conoce Ud. sobre el RansomWare? De ser así, sin mencionar el nombre de la Institución, fue su Institución o alguna otra que Ud. Conozca víctima de ello?

Sí conozco, se trata de un software que se aloja en el sistema operativo y cual parásito, toma la información personal y la copia a algún servidor en internet, donde su dueño/usuario puede tomar la decisión de permitir al virus el bloqueo de la computadora y exigir un dinero a cambio de su liberación, siendo a mi parecer un chantaje.

Conozco el caso de una empresa dedicada al service de tecnologías que fue víctima de ello y detuvo su producción hasta resolver el incidente, desconozco el tiempo y dinero invertido en ello hasta quedar resuelto.

9. ¿Opina Ud. Que la solución para evitar ser víctima sea adquirir antivirus más potentes a nivel personal/empresarial? En caso de que considere que no lo es, podría sugerir una solución?

No, estos delitos tienen fuerza sobre aquellos que están desinformados sobre estas modalidades, ya que de estar informados tendrían mas cuidado y sospecharían de cualquier tipo de mensaje por celular/correo/ etc. que no parezca fiable.

10. ¿Podría Ud. Listar las modalidades de ciberdelincuencia más comunes, así como también conocer su opinión sobre la cual Ud. Considere mas peligrosa y/o común?

Conozco el phishing que es suplantar la pagina real con la intención de engañar al usuario y almacenar datos privados como numero de tarjeta, fecha de vencimiento y cvv, y con ello proceder a realizar compras no autorizadas o simplemente cualquier tipo de transferencia, también puede ser una persona que se hace pasar

por otra con el fin de obtener tanta información como sea posible. Considero a ésta modalidad la más peligrosa pues mientras el ransomware ataca sobretodo a empresas, el phishing obtiene víctimas en todos los sectores.

Anexo 3: Ficha De Entrevista

Dirigido a especialistas en el ámbito de Derecho Penal

Título: Intervención de los órganos judiciales ante el aumento de amenazas de delitos informáticos durante el estado de emergencia por covid-19

Nombre del entrevistado: ENRIQUE LLONTOP SILVA

Edad: 36

Sexo: MASCULINO

Ocupación: ABOGADO

Fecha de la entrevista:

Entrevistador: Andy Antonio Ortiz Cahuana – Martin Leopol Adarmes Alvarez

Entrevistarlo respecto:

1.- ¿Teniendo en cuenta la coyuntura en la cual nos encontramos, que bienes jurídicos protegidos son vulnerados por los delitos informáticos?

Los delitos informáticos por su propia naturalexa son pluriofensivos o multiofensivos, ya que lesionan bienes jurídicos de información privilegiada, y bienes juridicidicos tales como la indenmidad sexual, la privacidad, el patrimonio o la fe pública.

2.- Según su experiencia ¿Desde la creación de la ley 27309 (Ley de delitos informáticos) y su derogación por la ley 30096 siendo modificada por la ley 30171, a la fecha no se ha visto una sentencia judicial que hable con respecto a estos delitos informáticos, a que cree que se deba esto?

Particularmente he advertido sentencias por delitos informáticos, pero no con apliación de la Ley vigente a la fecha, sino por aplicación remisiva a delitos especiales, emplo es el delito de hurto de dinero por transacciones bancarias, aquí se daría el supuesto para un delito informático al momento de la susracción de la

información de claves e información de tarjeta, sin embargo la investigación y posterior sentencia se da bajo la norma penal del Código Penal artículo 186.

3.- Se entiende por competencia judicial a todo ente encargado de actuar de manera técnica y jurídica en distintas instancias, conociendo la complejidad de estos delitos informáticos ¿cree usted que sea necesario crear una competencia judicial específica para el mejor entendimiento de estos delitos informáticos?

En realidad la delegación de facultades para investigar delitos informáticos si existe, tenemos la División de Delitos de Alta Tecnología de la PNP, es un organismo especializado para realizar investigaciones por la presunta comisión de delitos informáticos, luego de ello dicha investigación es derivada a la Fiscalia, considero que debé haber capacitación constante para los organismos ya existente.

4.- ¿Qué acciones considera usted que se deba optar por nuestros órganos de justicia para hacer frente a los delitos informáticos?

Debe haber más capacitación para identificar e investigar este tipo de delitos, asimismo debe haber campañas de sensibilización a manera de prevención.

5. ¿Considera Ud. que el Perú se encuentra en la capacidad jurídica de poder hacer frente a un ataque cibernético a entidades públicas y privadas?

Lamentablemente en el Perú no tenemos una tecnología avanzada, basta con solo ver el nivel de rapidez que tenemos en cuento a servicio de internet, que de por si es la peor de la Región.

6. ¿Considera Ud. Que el hosting de aplicaciones y la venta/uso de dominios con nomenclatura similar a marcas existentes deba ser regulado?

Definitivamente debe existir una regulación para su correcta aplicación y protección.

7. ¿Fue Ud. Testigo o víctima de la ciberdelincuencia? Sí fue así, cuál ha sido la consecuencia mental/laboral/personal en dicha persona luego de ser víctima de esta modalidad de delincuencia, sea compras no autorizadas por internet, retiro de dinero en nombre suyo sin consentimiento, etc?

Fui un testigo de oídas en delito informático de compras por internet, lamentablemente he visto como las víctimas en este tipo de delitos están totalmente

desprotegidas, no encuentran justicia, ya que ni siquiera la propia entidad bancaria que brinda la cuenta y tarjeta afectada quiere investigar, y obta por el facilismo, culpar al consumidor por no tener el deber de cuidado con la información de su tarjeta, cuando en muchas oportunidades el filtrado de información proviene desde el interior de la propia entidad bancaria.

8. ¿Conoce Ud. sobre el RansomWare? De ser así, sin mencionar el nombre de la Institución, fue su Institución o alguna otra que Ud. Conozca víctima de ello?

No he oído de ello.

9. ¿Opina Ud. Que la solución para evitar ser víctima sea adquirir antivirus más potentes a nivel personal/empresarial? En caso de que considere que no lo es, podría sugerir una solución?

Considero que es una forma de menguar y protegerse ante posibles delitos informáticos, todo acto de prevención es útil.

10. ¿Podría Ud. Listar las modalidades de ciberdelincuencia más comunes, así como también conocer su opinión sobre la cual Ud. Considere mas peligrosa y/o común?

Sustracción de información privilegiada, hurtos cibernéticos, compras por internet con tarjetas clonadas, delitos contra la libertad sexual, suplantación de identidad con la finalidad de estafar a personas ofreciendo productos de empresas que no existen, etc.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad de los Autores

Nosotros, ADARMES ALVAREZ LEOPOL MARTIN, ORTIZ CAHUANA ANDY ANTONIO estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "INTERVENCIÓN DE LOS OPERADORES DE JUSTICIA ANTE EL AUMENTO DE AMENAZAS DE DELITOS INFORMÁTICOS DURANTE EL ESTADO DE EMERGENCIA POR COVID-19", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
ANDY ANTONIO ORTIZ CAHUANA **DNI:** 71080243 **ORCID** 0000-0001-6098-4249	Firmado digitalmente por: AORTIZC67 el 21-12-2020 12:40:27
LEOPOL MARTIN ADARMES ALVAREZ **DNI:** 74831457 **ORCID** 0000-0002-0003-5663	Firmado digitalmente por: LADARMESA el 21-12-2020 19:57:17

Código documento Trilce: TRI - 0091046

INVESTIGA UCV