UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE **DERECHO Y CIENCIAS POLÍTICAS.**

"LAS MEDIDAS DE SEGURIDAD Y LA INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN LA REGULACIÓN PERUANA 2021 - 2022"

Tesis para optar al título profesional de:

ABOGADA

Autor:

Jessica Marilu Melgarejo Solorzano

Asesor:

Mg. Michael Lincold Trujillo Pajuelo
https://orcid.org/0000-0002-0757-2349

Lima - Perú

2023

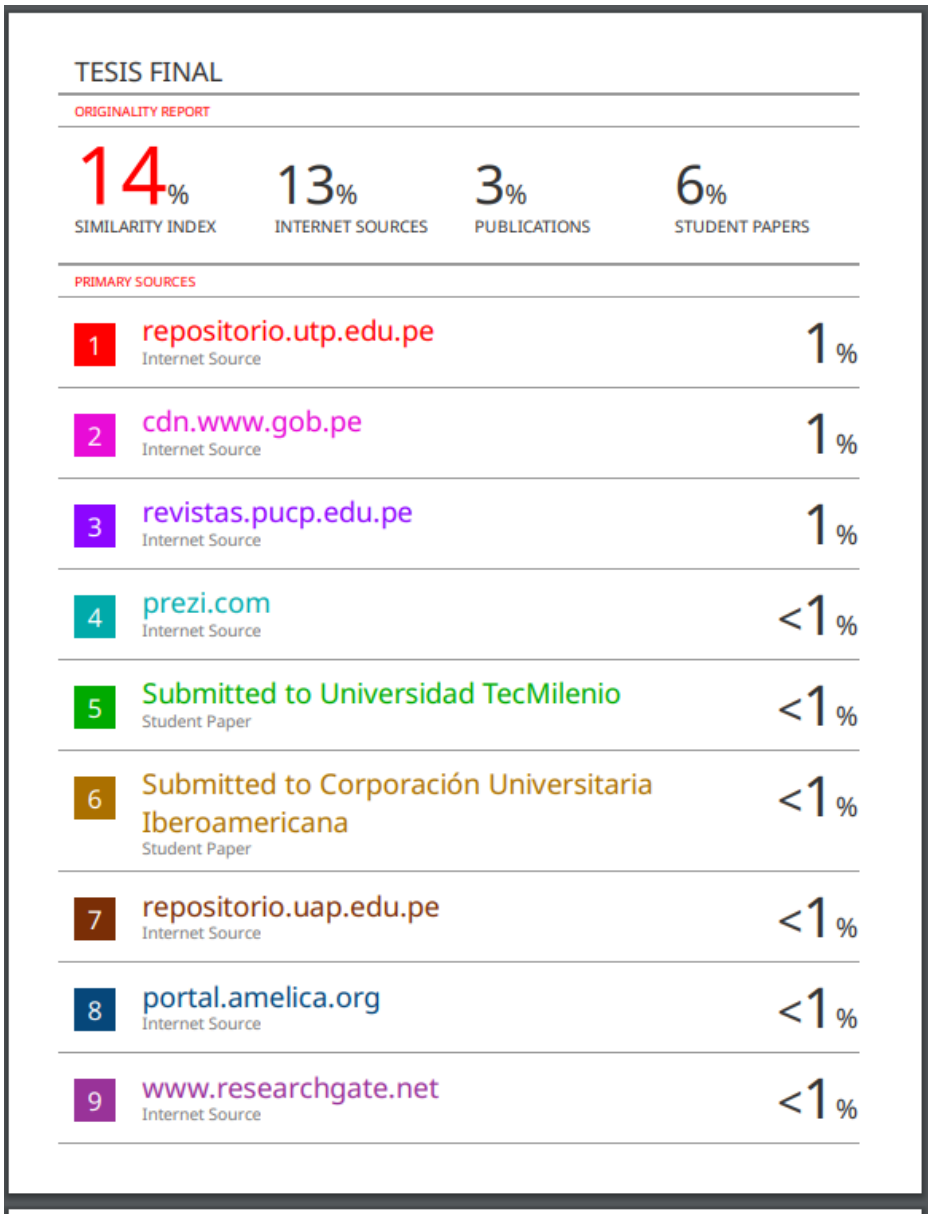
JURADO EVALUADOR

Jurado 1 Presidente(a)	**NOE VALDERRAMA MARQUINA** Nombre y Apellidos

Jurado 2	**VANESSA ANTHUANET VIGIL RUIZ** Nombre y Apellidos

Jurado 3	**MICHAEL LINCOLD TRUJILLO PAJUELO** Nombre y Apellidos

INFORME DE SIMILITUD



TESIS FINAL

ORIGINALITY REPORT

14%	13%	3%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repositorio.utp.edu.pe Internet Source	1%
2	cdn.www.gob.pe Internet Source	1%
3	revistas.pucp.edu.pe Internet Source	1%
4	prezi.com Internet Source	<1%
5	Submitted to Universidad TecMilenio Student Paper	<1%
6	Submitted to Corporación Universitaria Iberoamericana Student Paper	<1%
7	repositorio.uap.edu.pe Internet Source	<1%
8	portal.amelica.org Internet Source	<1%
9	www.researchgate.net Internet Source	<1%

DEDICATORIA

A mi bella hija, por ser el motor y motivo en mi vida, a mi pareja por su apoyo incondicional y no dejarme vencer por los obstáculos.

A mis padres, por su apoyo, compañía y cariño durante esta etapa.

AGRADECIMIENTO

A mis padres por su apoyo constante y a mi compañero de vida por estar conmigo en las buenas y en las malas, por brindarme su apoyo constante y no dejarme sola en los momentos más difíciles.

Tabla de contenido

JURADO CALIFICADOR **2**

INFORME DE SIMILITUD **3**

DEDICATORIA **4**

AGRADECIMIENTO **5**

TABLA DE CONTENIDO **6**

ÍNDICE DE TABLAS **7**

ÍNDICE DE FIGURAS **8**

RESUMEN **9**

CAPÍTULO I: INTRODUCCIÓN **11**

1.1. Realidad problemática 11

1.2. Formulación del problema 22

1.3. Objetivos 22

1.4 Hipótesis 22

1.5 Justificación 23

CAPÍTULO II: METODOLOGÍA 24

CAPÍTULO III: RESULTADOS 33

CAPÍTULO IV: DISCUSIÓN Y CONCLUSIONES 44

REFERENCIAS 49

ANEXOS 52

ÍNDICE DE TABLAS

Tabla 1. Población a entrevistar 26

Tabla 2. Entrevistado e información académica del entrevistado 28

Tabla 3. Ley N° 30096 30

Tabla 4: Objetivo general 33

Tabla 5: Objetivo específico 1 35

Tabla 6: Objetivo específico 2 37

Tabla 7: Preguntas para los entrevistados 40

ÍNDICE DE FIGURAS

Figura 1. Hogares que acceden a internet 20

Figura 2. Hogares que cuentan con un celular 21

Figura 3. Denuncias del año 2013 al 2020 43

RESUMEN

La investigación se centra en el tema de medidas de seguridad y la interceptación de datos informáticos en la regulación peruana 2021-2022. Para ello se recaudó información de la base de datos de Dailnet, Scielo, Google académico, Redalyc, Ebsco, Repositorio Univ4ersitario en el idioma español, las cuales fueron seleccionadas para responder a la pregunta de investigación, ¿De qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022? Y así poder llegar a nuestro objetivo de determinar de qué manera las medidas de seguridad limita la interceptación de datos informáticos en la regulación peruana 2021-2022. Además de realizar el análisis de la mencionada ley, también se realizó 8 entrevistas, las cuales se realizaron a abogados en el área penal, fiscales y juez quienes dieron su opinión propia sobre el tema y que consideran que a pesar de ser aplicada la ley N°30096 los delitos siguen en aumento, por lo cual no se ve ninguna disminución desde que se aprobó esta ley.

Con todo lo analizado lo que se busca es demostrar que los casos de interceptación de datos informáticos siguen en aumento, que a pesar de que exista una ley, no significa que eso es la solución, quizás porque la sanción no es severa que no causa temor a los delincuentes que siguen cometiendo el delito mencionado y a raíz de esto producen otros delitos en las cuales no solo se perjudican los adultos, sino también los menores de edad.

PALABRAS CLAVES: Interceptación de datos informáticos, medidas de seguridad, protección de datos personales, seguridad de datos informáticos.

ABSTRACT

The information was collected from the database of Dialnet, Scielo, academic Google, Redalyc, Ebsco, Repositorio Univ4ersitario in the Spanish language, which were selected to answer the research question, ¿How do security measures limit the interception of computer data in the Peruvian regulation 20121-20122? And thus be able to reach our goal of determining how security measures limit the interception of computer data in Peruvian regulation 2021-2022. In addition to carrying out the analysis of the aforementioned law, 8 interviews were also carried out, which were carried out with lawyers in the criminal area, who gave their own opinion on the subject and who consider that despite the application of Law N°. 30096, the Crimes are still on the rise, so no decrease is seen since this law was passed.

With everything analyzed, what is sought is to demonstrate that cases of interception of computer data continue to increase, that despite the existence of a law, it does not mean that this is the solution, perhaps because the sanction is not severe and does not cause fear. To criminals who continue to commit the aforementioned crime and as a result of this they produce other crimes in which not only adults are harmed, but also minors..

KEYWORDS: Computer data interception, security measures, personal data protection, computer data security.

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

Hoy en día en todo el mundo las personas usan el internet como medio de comunicación y muchas veces comparten sus datos personales sin tomar precauciones o medidas de seguridad por lo que se da el robo de información de datos personales, esta se da por medio de la intercepción de los datos informáticos, es decir que los datos que se comparten son interceptados y usados sin la autorización de la persona afectada.

El autor Nevárez (20017), en su artículo "*robo de información, más común de lo que creen"* indica que las redes sociales han sido un gran impacto ya sea de manera positiva o negativa en cuanto a la vida cotidiana, ya que son útiles al momento de contactar amigos o de reencontrarse con viejos conocidos de la infancia, pero a su vez son bastante peligrosas ya que se tiene la costumbre de publicar todo lo que hacemos. Es decir que, al poner hasta la mínima información personal, hacen que sean más vulnerables a que puedan interceptar la información, por lo que se debe tener cuidado con lo que se coloca como información.

También nos dice que la información puede ser fácilmente violada o vulnerada por personas que desean hacer un daño, no necesariamente tienen que ser hackers, sino personas comunes con aires de delincuente robándole información a gente común descuidada con la que pueden desde suplantar identidad, hasta efectuar un secuestro o algo mucho peor.

Según Alvarado (2016) en su artículo "*la gestión de la seguridad de la información en el régimen peruano de protección de datos personales*", nos dice que el tratamiento informático de datos al mantener, dar, hacer impenetrable o propagar la información en forma instantánea e ilimitada en el espacio provoca el aumento del riesgo de seguridad.

La sociedad misma pone la información al alcance de los delincuentes que están dispuestos a tomar la información compartida para su beneficio propio, muchos de los que utilizan el internet lo hacen sin ninguna seguridad y comparten sus datos con personas desconocidas que muchas veces se hacen pasar por personas que nos son.

En nuestra legislación tenemos La Ley N° 30096 "Ley de Delitos Informáticos" en esta ley podemos ver cuáles son las penas que existen para el delito de intercepción de datos informáticos, así mismo podemos observar que a través de este delito se llegan a cometer muchas más, para las cuales las penas también son diferentes dependiendo la gravedad del delito que se cometió.

En esta investigación también se observará qué criterios se toman para dar una sanción a los sujetos que cometen el acto de interceptación o robo de datos informáticos. Asimismo, saber cómo se puede evitar este tipo de delito ya que una vez que lo realizan, perjudican a la persona que pertenecen los datos interceptados, asimismo veremos cuáles son las medidas de seguridad que podemos adoptar para la protección de la información que se comparte en el internet.

Antecedentes Nacionales

Según Alvarado (2016) en su artículo "*la gestión de la seguridad de la información en el régimen peruano de protección de datos personales*", indica que la seguridad de la información es uno de los temas principales establecidos en la ley de protección de datos personales, la que es una obligación de los propietarios y de quienes están encargados de los bancos de datos personales además de todo lo relacionado con el tratamiento de datos personales. Este autor hace mención a que no solo la responsabilidad es de la persona que comparte información, sino que también son responsables los que manejan los bancos de datos y todos los que tengan que ver con ellos, es decir que no solo a las personas pueden

interceptar la información sino también al banco de datos en la cual se encuentran información y por el manejo incorrecto se da la interceptación de datos informáticos.

Según Castro, Moran y Navarrete (2018) en su artículo "*Introducción a la seguridad informática y el análisis de vulnerabilidades*" indica que la principal tarea de la seguridad informática es la de reducir los riesgos, pero estos vienen de diferentes lugares, puede ser al momento de ingresar los datos, es decir el medio que transporta la información, del hardware que es usado para transferir y aceptar los datos, pero el objetivo principal es disminuir los riesgos para obtener mejor y mayor seguridad. Es decir, con el pasar de los años la tecnología ha avanzado, también las medidas de seguridad, es cuestión de que cada ciudadano tome conciencia sobre los riesgos que tiene al proporcionar datos personales en la red. No se puede decir que la tecnología este demás, sino todo lo contrario, nos ayuda en nuestra vida cotidiana, pero a su vez nos pone en situaciones peligrosas, se puede evitar conociendo las medidas de seguridad que existen para el internet.

Según Ocampo (2017) El aumento constante del mercado negro de la información, funciona como mecanismo que instiga a una importante masa de ataques informáticos, principalmente destinados a conseguir bases de datos con información personal (pág.10-11). Este autor hace mención a un mercado negro de información, es decir que estos mercados pagan por adquirir información, si no existiera estos mercados quizás los delincuentes no les interesaría tanto interceptar información, ya que no sacarían mucho beneficio de ello, es decir nadie les pagaría por esta información.

Según Terreros (2015) La sociedad de la información ha hecho minimizar notablemente y hasta ha eliminado el valor y la importancia de la territorialidad (pág.3). Es cierto que con el avance de la tecnología también la delincuencia ha avanzado, es decir que

al realizar un delito informático no es necesario que el delincuente este en el mismo lugar que su víctima, este incluso podría estar en otro país y aun así estaría cometiendo el delito.

Antecedentes Internacionales

Según Rodríguez (2018) El aumento acelerado en el uso de dispositivos tecnológicos como equipos portátiles, teléfonos inteligentes, tablets, no solo surge como un fenómeno de carácter tecnológico, sino también como una manifestación de comportamiento. Este autor hace mención que hoy en día la sociedad usa dispositivos como medio de comunicación, a su vez por medio de ellos comparten información, esto ya se ha vuelto una costumbre, es decir es un comportamiento que se tiene y no lo pueden dejar, ya que forma parte de la vida diaria.

Según Ferrer (2017) en su artículo "*Protección de datos/privacidad en la época del big data*" indica con la protección de datos personales da la sensación de resguardar los datos personales, pero en realidad protege a las personas con las que esos datos están relacionados, es decir a los sujetos afectados (pág. 24). Este autor nos dice que la protección de datos es para la persona, es decir para quien sufre el daño, en realidad se protege al sujeto que saldrá afectado con la interceptación de datos informáticos.

Según Pino (2016) en su libro "*Delitos informáticos*" indica que esta dependencia de la sociedad a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace evidente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden producir en la vida cotidiana (pág.5).

Es cierto que la sociedad de hoy en día depende mucho de la tecnología, ha comparación con años anteriores, la tecnología ha ido evolucionando más que los seres

humanos. Este avance de tecnología en parte nos es útil, pero a su vez nos perjudica y se producen delitos. Por más cuidadoso que sea la sociedad siempre habrá un avance tecnológico que no se pueda manejar adecuadamente.

Según Elneser y Santamarina (2012) El delito informático no se relaciona solo a una modalidad de tipo penal sino a una variedad de conductas que pueden y deben ser tipificados de manera independiente. Es claro que la persona que comete un delito por medio de la interceptación de datos informáticos realiza diversos comportamientos para elaborarlo, tenemos como la vulneración a la privacidad, es decir que sin permiso de nadie está obteniendo información que no es compartida con nadie.

Según Fonseca (2021), Con el inminente auge de la globalización, el cual vino de la mano con otro gran fenómeno informático, como lo fue el internet emergieron como protagonistas la virtualidad y lo digital, con lo que se eliminaron las barreras locales y transicionales (pág. 5). Es claro que la tecnología ha evolucionad con el transcurso del tiempo, antes para que uno se comunique se tenía que enviar cartas cuando se trataba de lugares lejanos, pero ahora no si tienes una computadora e internet puedes comunicarte con personas de otro país sin necesidad de enviar cartas y esperar respuesta por días, ahora con el internet todo es inmediato, muchas veces no se tiene control de la información que se comparte, se hace sin pensarlo, peor aún si lo comparten adolescentes, la sociedad debe ser responsable al momento de usar la tecnología ya que esta es de mucha ayuda en la vida cotidiana pero a su vez puede causar mucho daño.

Los autores Acosta, Benavides, y Patricio (2020) indican que la información puede ser cualquier tipo (personal, empresarial, financiera-bancaria, societaria) siendo buscado por los conocidos delincuentes informáticos con el propósito de obtener un beneficio lucrativo, por intermedios de chantaje, desprestigio y hasta secuestro informático. Es decir, que

cualquiera puede ser víctima de la interceptación de datos informáticos, hasta incluso las empresas o bancos, los delincuentes que llegan a interceptar estos datos pueden usarlo para sacar ganancia y se realiza con conocimiento de los actos y el daño que provocan a su víctima.

Estos autores nos hacen mención de que no solo nuestro país esta vulnerable a la interceptación de datos informáticos sino también el resto del mundo y los delincuentes se aprovechan de los avances de la tecnología para robar la información que se comparte y hacer uso de ella con la finalidad de obtener su propio beneficio, asimismo la protección de datos solo protege a las personas que son afectadas y no protegen a los datos compartidos, por lo que depende de cada uno tener cuidado a quien se le comparte nuestra información y donde se comparte.

Marco teórico

Bases teóricas

Método cualitativo

Según Valladolid y Chávez (2020), Los métodos cualitativos centran su interés en los escenarios naturales y reales en los que los seres humanos interaccionan y se desarrollan. Asimismo, el autor señala que este tipo de investigación son adecuadas para analizar los problemas jurídicos y cuestiones jurisprudenciales. Es decir que este tipo de métodos está enfocado a los hechos reales que suceden en el día a día, en las cuales participan los seres humanos. El método cualitativo se concentra en la descripción e interpretación de las situaciones que se den en el entorno de la sociedad.

Método cuantitativo

El método cuantitativo está enfocado en números y se aplica al final de un proyecto, es decir que este método lo usan más las personas que aplican estadísticas a sus investigaciones mientras que la anterior no es así.

Interceptación de datos informáticos

La Ley N° 30096 hace referencia que, a través de la tecnología, se llega a interceptar datos informáticos en transmisiones no públicas, es decir transmisiones privadas las cuales son dirigidas a un sistema informático. Es claro que la ley considera que todo acto delictivo realizado con la tecnología se da por la interceptación de datos, asimismo que con transcurso de los tiempos la tecnología ha ido evolucionando y con ello los métodos que usan los delincuentes han ido mejorando de igual manera. El avance de la tecnología tiene sus pros y contra en el mundo, esto depende de cómo manejemos nuestra información.

Seguridad de datos informáticos

Según Ticona & Mamani (2018), la seguridad de datos informáticos es la agrupación de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que ayudan a proteger la información personal con la finalidad de mantener la confidencialidad e integridad de datos, (Ticona & Mamani, 2018), este autor nos indica que son medidas preventivas para cuidar y proteger nuestra información de los delincuentes que pretendan interceptar nuestros datos informáticos, los cuales lo realizan con el único fin de lucrar con nuestra información y sacar un beneficio propio.

Según Coppola (2023), la seguridad informática es la agrupación de tecnologías, procesos y prácticas las cuales están destinadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado se

produzca,. Así como la tecnología ha evolucionado con el transcurso de los tiempos, lo mismo ha pasado con la seguridad informática, existen muchos métodos de protección para la información que proporcionamos en la red, se puede evitar los hackers, entre otros, todo esto depende de cada uno para proteger su información y evitar que perjudiquen de alguna manera nuestra privacidad.

Banco de datos

Alvarado (2016) nos dice en su artículo “*La gestión de la seguridad de la información en el régimen peruano de protección de datos personales*”, indica que los bancos de datos es la unión organizada de datos personales, cualquiera fuere la estructura o modalidad de su creación, formación, almacenamiento, organización y acceso. El autor indica que la base de datos son todos nuestros datos recopilados y organizados para estar almacenados, pero muchas veces esto no sucede ya que con el avance de la tecnología los delincuentes cibernautas interceptan estos datos para luego usarlo a su propio beneficio.

Redes sociales

Según Hiitt quien cita a Celaya (2008) en su artículo “*Las Redes Sociales: Una Nueva Herramienta de Difusión”*, las redes sociales son lugares en internet donde las personas comparten y publican todo tipo de información, personal y profesional, con terceras personas, ya sean conocidos y absolutos desconocidos (pág. 04).

Queda claro que sin importar la distancia o el lugar que uno se encuentra se puede comunicar con quien desee por las redes sociales, a través de esto conocemos a personas que se encuentra a kilómetros de nosotros, ya sean de otro distrito, capital, país, etc. Es decir que se puede conocer a nuevas personas sin la necesidad de que las estés viendo, o estar frente a frente.

Tecnología

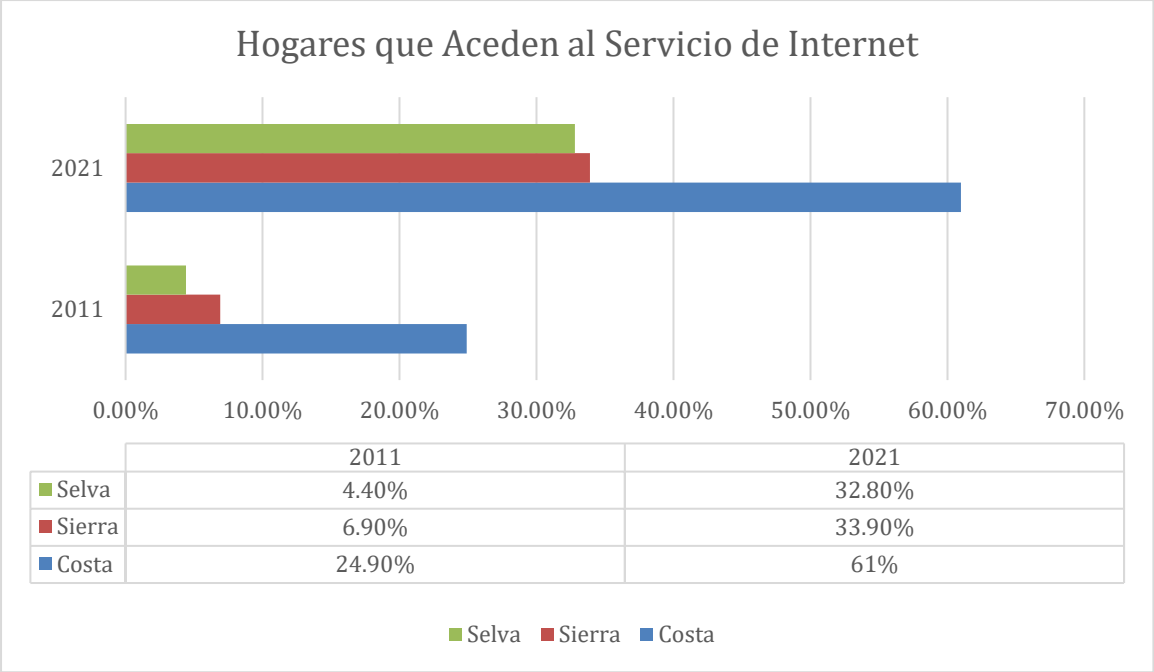
Según Cueto, Hernández y Argandoña (2020) en su artículo *“Tecnologías de información: acceso a internet y brecha digital en Perú*”, la tecnología está en todos los aspectos de nuestra vida diaria de tal manera que no existe un momento sin ella. La época en que vivimos, es la era de la tecnología, ya que la mayor parte de los seres humanos viven altamente influenciados por la tecnología, y en una interacción continua de la misma (pág.505). Como lo menciona lo citado, la tecnología está presente en la vida cotidiana las 24 horas del día y los 7 días de la semana, actualmente en la sociedad la tecnología es usada por menores de edad, así como por adultos, no hay en ningún momento que alguien este sin un celular en la mano, la tecnología ha evolucionado tanto que hoy en día tenemos al internet en la palma de nuestra mano por medio de un celular.

Internet

Según el sitio web Enciclopedia Humanidades (2023), “el internet es la red que conecta y relaciona dispositivos electrónicos y redes de computadoras entre sí, es decir no importa la distancia, conecta a todo el mundo. Además, es una red informática de telecomunicaciones que tiene un sistema de reglas para las conexiones entre diferentes dispositivos y estas resulten compatibles”.

Es decir, el internet permite comunicarse en el momento con persona que se encuentren lejos sin la necesidad de estar enviando una correspondencia y esperar días para una respuesta. Hoy en día la sociedad de alguna manera se mantiene en línea (conectado en internet) ya sea por medio de una laptop, Tablet, computadora o celular.

Figura 1

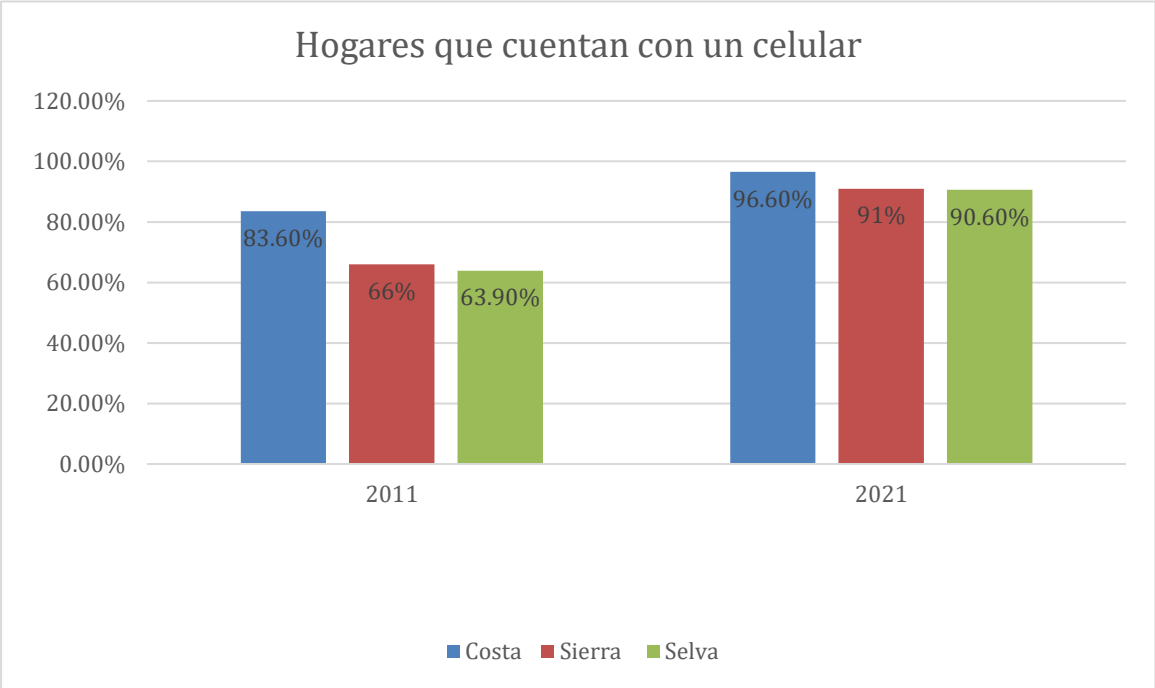


	2011	2021
Selva	4.40%	32.80%
Sierra	6.90%	33.90%
Costa	24.90%	61%

Fuente: elaboración propia con información de INEI

En la figura presentada se puede observar el aumento de tener internet en casa ha aumentado en los últimos años, como se aprecia en el cuadro tenemos costa, sierra y selva, las cuales han aumentado de manera alta. Se observa que la selva tuvo un incremento de 28.4% en el acceso a internet, mientras que en la región de la sierra se tuvo un incremento del 27% y por último la costa quien incremento en un 36.1% de su acceso al internet, el aumento es muy notorio entre los últimos años según la información brindad por el INEI. El uso de tener internet en casa hoy en día es necesario por el mismo hecho de que ahora existen trabajos remotos, el cual fue el más usado durante la pandemia del covid-19 por lo que la sociedad necesitaba contar con internet en casa para poder laborar, también para las clases remotas que hubo, tanto para colegios y universidades estatales como particulares.

Figura 2



Fuente: elaboración propia con informacion del INEI

Como se puede apreciar en el cuadro, ya sea en la costa, sierra o la selva siempre hay algún familiar que tiene un celular el cual le permite estar conectado a internet y proporcionar su información personal, si bien es cierto hoy en día no solo los adultos usan un celular sino los menores de edad también y muchas veces lo usan sin supervisión de un adulto. Según la información de INEI en los últimos años hubo un incremento del 13% en la costa, mientras que en la sierra 25% y en la selva 26.7%, se ´puede observar que en la regios de la selva y la sierra hubo mayor incremento que en la costa, en tener algún familiar del hogar con celular.

Es claro que contar con un celular hoy en día significa estar conectada al internet, los celulares de hoy no son como antes, ahora es un aparato delgado, plano pero que cuenta con muchos usos para navegar en la red, cuando antes no se podía usar más que para llamadas.

1.2. Formulación del problema

1.2.1 Problema General

¿De qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022?

1.2.2 Problemas Específicos

_ ¿Cuáles son las medidas de seguridad adoptadas por la regulación peruana en la interceptación de datos informáticos?

_ ¿Cuáles son las sanciones adoptadas por la regulación peruana para el delito de interceptación de datos informáticos?

1.3. Objetivos

1.3.1 Objetivo General

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022

1.3.2 Objetivos Específicos

_ Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos.

_Determinar las sanciones adoptadas por la regulación peruana para el delito de interceptación de datos informáticos.

1.4. Hipótesis

1.4.1 Hipótesis General

Las medidas de seguridad limitan a la interceptación de datos informáticos al momento que la sociedad comparte información personal.

1.4.2 Hipótesis Específicos

_Las medidas de seguridad usadas por la regulación peruana ayudan a la sociedad a mantener a salvo los datos personales que comparten diariamente.

_Las sanciones adoptadas por la regulación peruana se encuentran tipificados en la ley N° 30096 en la que se observa que por medio de este delito se ocasionan otros delitos que perjudica a la sociedad.

1.5 Justificación de la Investigación

Esta investigación se realizó con el fin de conocer las medidas de seguridad que adopta la regulación peruana frente a la interceptación de datos informáticos, así como también conocer las sanciones que se imparten por este delito, las cuales se encuentran en la ley N° 30096, por otro lado en esta ley se puede observar que por producto de la interceptación de datos informáticos se ocasionan delitos que pueden hasta amenazar la vida e integridad de la persona quien compartió sus datos personales.

También esta investigación nos mostrara como las medidas de seguridad influyen en las personas, si son usadas adecuadamente por la sociedad, también investigar que otras medidas se pueden adoptar con el único fin de proteger la información personal de cada persona.

CAPÍTULO II: METODOLOGÍA

2.1 Tipo de Investigación

Enfoque

Según Valladolid Nizama y Chávez Nizama (2020) en su libro "*El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis*" nos indica que el interés del enfoque cualitativo se centra en los escenarios naturales y reales en los que los seres humanos se relacionan y se desenvuelven, es decir que este tipo de investigación se realiza en un escenario real con hechos sucedidos anteriormente que sirven como base para una investigación. Por ende, el tipo de investigación que se realizó en el presente trabajo es cualitativo

Asimismo, Cotán (2016) en su artículo "El estudio de la investigación cualitativa ", el investigador tiene que focalizarse en dar respuesta a las preguntas de investigación planteada a partir de las experiencias reales de las personas. Es decir que a bases de las experiencias reales se realizan las cuestiones de investigación las cuales tendrán una respuesta en base a los hechos reales.

Además, este tipo de estudio es utilizado para obtener una comprensión profunda y adecuada de los problemas que se manifiestan en el entorno de la sociedad.

Tipo

Para Otero (2018) La investigación cualitativa se fundamenta en la observación y evaluación de los fenómenos estudiados, realizando conclusiones de lo hallado en la realidad estudiada, asimismo este tipo de investigación permite realizar encuestas, entrevistas, descripciones y punto de vista de los investigadores. Es decir que por medio de esta

investigación se puede realizar entrevista, encuestas, etc. con el fin de llegar a una conclusión de todo lo observado y evaluado en la investigación.

Diseño

Para el desarrollo de este trabajo se consideró que los diseños a utilizar serian la teoría fundamentada y el análisis de casos, siempre y cuando dichas reflexiones lleven al logro de los objetivos antes mencionados, así mismo se realizó entrevistas para adquirir información sobre el tema investigado.

Teoría fundamentada

Según Hernández, Herrera, Martínez, Páez J., y Páez M. (2011) La Teoría Fundamentada es una de los hábitos de investigación cualitativa, la cual permite formular una teoría que se encuentra oculto en la información obtenida en el campo experimental. Además, emplea técnicas de investigación cualitativa como: la observación, las entrevistas a profundidad, la realización de memos, entre otras. Es decir que por medio de esta teoría podemos formular una teoría y emplear técnicas de investigación que ayudara a la realización de la investigación para lograr el objetivo antes mencionado.

La presente investigación usa la teoría fundamentada como diseño para ser desarrollado, siempre y cuando se cumpla con explicar mediante la recopilación de documentos y análisis a través de la experiencia con respecto al tema de interceptación de datos informáticos y las medidas de seguridad en la regulación peruana en el periodo 2021-2022.

Análisis del caso

Según Martínez (2006) El método de estudio de caso es una estrategia metodológica de investigación científica, es útil en la procreación de resultados que posibilitan el

crecimiento y desarrollo de las teorías existentes o al aparecer nuevos paradigmas científicos; por lo tanto, ayuda al desarrollo de un campo científico establecido.

Por lo tanto, este diseño reforzara de forma analítico el entorno al tema tratado, aumentando de esta manera la evidencia formulada con el análisis de datos para obtener el objetivo de esta investigación.

2.2 Población y muestra

Para Toledo (2016) en su artículo "*Población y muestra*", La población es el conjunto de personas u objetos a los que se quiere investigar, mientras que la muestra es la agrupación de unidades o elementos de análisis sacados del marco muestral o directamente de la población, es decir que muestra es parte de la población, ya que esta son unidades de la población.

En la presente investigación, la población utilizada durante la composición del proyecto fueron un conjunto de 8 elementos, 7 personas entrevistadas y análisis de la ley 30096; sin embargo, el ingreso de nuevo material documental quedara abierto para su inclusión durante el proceso de investigación de acuerdo a los criterios que configuran la naturaleza de esta investigación.

Los entrevistados son abogados penalistas, juez, fiscal y docentes penalistas que ven netamente el ámbito penal y se encuentran relacionados al tema de investigación.

Tabla 1

Población	Criterio	Instrumento	Tiempo de experiencia

Personal encargado de la fiscalía penal del callo	Abogada penalista, actualmente fiscal en el distrito del callao	Guía de entrevista	10 años como abogada y 3 como fiscal
Personal encargado de la fiscalía penal del callo	Abogada penalista, actualmente especialista en el distrito de callao	Guía de entrevista	5 años como abogada y 2 como especialista
Personal de caro y asociados	Abogado penalista	Guía de entrevista	2 años como abogado
Docente y abogado penalista	Docente en la UPN	Guía de entrevista	
Juez de la corte superior de justicia del callao	Juez	Guía de entrevista	2 años como juez
Abogado y docente de la escuela de sub oficiales de la	Docente y abogado	Guía de entrevista	5 años como docente de la escuela

PNP-puente piedra			de sub oficiales y 3 como abogado
Personal fiscal encargado de la fiscalía penal del callo		Guía de entrevista	2 años como fiscal

Fuente: Elaboración propia

En la tabla 1 se presenta a la población que se pretende entrevistar, mediante una guía de entrevista, con la finalidad de conocer sus opiniones para luego ser comparadas. Con la ayuda de sus opiniones se podrá llegar a una conclusión para cada objetivo.

Tabla 2

ENTREVISTADOS	DESCRIPCIÓN
Avelino Confesor Chupillón Vega	Abogado de profesión y docente en la escuela de sub oficiales de puente piedra
Delia Yenny Juárez Neyra	Fiscal Adjunta Provincial de la Octava Fiscalía Provincial Penal Corporativa del Distrito Fiscal del Callao.

Claudia Lluen Espino	Fiscal Adjunta Provincial de la Primera Fiscalía Provincial Penal Corporativa del Distrito del Callao
Liliam Patricia Chuquiruna Atencio	Maestría en Derecho Penal en la Universidad de Jaén-España Fiscal adjunto del Décimo Primera Fiscalía Provincial Penal Corporativa del Callo.
Renzo Jesús Vásquez Villacorta	Abogado de la universidad privada del norte. Abogado penalista y docente.
Fernando Ikehara Véliz	Abogado y socio de pazos Ikehara Abogados. Docente de derecho en la Universidad Privada del Norte y la Universidad Científica del Sur
Azucena Yenny Tolentino Galindo	Juez del Octavo Juzgado de Investigación Preparatoria Permanente de la Corte Superior de Justicia del Callao

Fuente: elaboración propia

En la tabla 2 se observa quienes son las personas que serán entrevistadas y a su vez información de ellos, todos los entrevistados son especialistas en materia penal, son abogados, fiscales, docentes y jueza, a quienes se les realiza la entrevista

para conocer sus opiniones sobre el tema de investigación.

Tabla 3

N° DE LEY	AÑO DE PUBLICACIÓN
Ley N° 30096 – ley de delitos informáticos	27 de septiembre 2013

Fuente: Elaboración propia

2.3 Técnicas e instrumentos de recolección y análisis de datos

Se realizará un análisis de las entrevistas realizadas para obtener información sobre el tema de investigación como se explica en lo siguiente:

El estudio documental es una intervención intelectual que da lugar a un subproducto o documento secundario que hace como intermediario o instrumento de búsqueda obligado entre el documento original y el usuario que solicita información, (Castillo, 2015). Esto quiere decir que su finalidad es la recopilación de datos, para obtener nuestro objetivo en la investigación.

En este sentido, el proyecto de investigación se focaliza en la recopilación de las respuestas dadas por las personas entrevistadas, estas entrevistas están enfocadas en la interceptación de datos informáticos y las medidas de seguridad para evitarlas.

Según Raffino (2020) La entrevista es un intercambio de ideas u opiniones que se realiza en una conversación, la cual se da entre dos o más personas. En ella **se** hacen preguntas que antes fueron pensadas y lo realizan a un entrevistado en particular, quien responde concretamente la pregunta y da su opinión. Es decir que esta técnica nos permite

conocer la opinión de la otra persona, de esta manera nos permite a dialogar y dar puntos de vista respecto al tema tratado.

Para establecer los objetivos de esta investigación se realizó mediante la técnica de análisis documentales, la cual será uno de los instrumentos cuyo uso se hará presente, ya que ayudara en la organización y selección de documentos, las cuales deben ir en armonía con los objetivos de la investigación.

Al igual que las guías de análisis documental, el instrumento de guía de entrevistas será una importante herramienta de guía y organización, la cual ayudará a la recolección de datos de profesionales entrevistadas con respecto al tema de investigación.

2.4 Procesamiento y análisis de datos

El procesamiento y el análisis da datos se llevó a cabo mediante una entrevista a 7 abogados los cuales son: 1 juez del ámbito penal, 3 fiscales penalistas, 2 abogado y profesor penalista, 1 abogado especialista en litigación. Así como el análisis de la ley 30096 que nos habla sobre las penas que reciben las personas que cometen el delito de interceptación de datos informáticos.

Para la recolección de las entrevistas no fue nada sencillo, se tuvo que realizar las preguntas de la entrevista de acuerdo al tema de investigación y los objetivos que se quería llegar, una vez realizadas las preguntas se tuvo que buscar a personas relacionadas al tema, lo cual no fue nada sencillo, se enviaron correos para que cada uno aceptara a ser entrevistado e indicaran que día podría realizarse la entrevista. Hubo algunos que aceptaban, pero al momento de llegar el día de la entrevista me cancelaban por lo que me tomo mas tiempo seguir buscando, tanto así que los que, si pudieron, no contaban con tiempo para realizarlo

de manera virtual o presencial, por lo que se tuvo que enviar la entrevista como un documento para que ellos lo lleguen a contestar y me lo envíen.

De esta manera es como se llego a obtener la información proporcionada a la investigación.

El método inductivo va desde la vivencia hacia la idea abstracta, la idea abstracta o indeterminado es la teoría o los conceptos, por otro lado, la vivencia o experiencia son los pensamientos, las vivencias, la percepción y opinión del sujeto que ha vivido desde el quehacer cotidiano ya sea laboral, profesional u otro campo, (Palmet Urzola, 2020). Es decir que esta investigación utilizara este método la cual está referida a una indagación de lo particular a lo general, respetando la opinión de cada entrevistado.

Las entrevistas se realizaron siempre manteniendo un respeto a hacia las personas entrevistadas, buscando un bien en común, es decir que tanto los entrevistados como la entrevistadora buscan hacer conocer mas sobre el tema y como es o que idea tienen sobre este tema los profesionales que se llego a entrevistar en esta investigación.

CAPÍTULO III: RESULTADOS

Es relevante para la presente investigación, señalar que las entrevistas realizadas fueron a abogados penalistas, fiscales en el ámbito penal que ven todo tipo de casos en su día a día, así como también el presente tema de investigación.

Esto se realizó con el único fin de dar respuesta al tema de investigación y a su problemática, la cual es: de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021-2022.

En base a los entrevistados antes mencionados (tabla 2) se puede llegar a la conclusión que cada uno de ellos tienen una opinión no tan desacuerdo, analizaremos las respuestas para cada objetivo que dieron los entrevistados a continuación:

Objetivo General: Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021-2022.

A continuación, se muestra una tabla, la cual contiene el nombre del entrevistado y su respuesta:

Tabla 4

ENTREVISTADO	RESPUESTA
TOLENTINO (2022)	La interceptación de datos informáticos en el Perú se da por la falta de tener cuidado con quienes se expone nuestra información personal, además del mal uso de las medidas de seguridad que existe, no solo depende de estas medidas si no de uno mismo, las medidas de seguridad no minimizan la interceptación de datos, al contrario por cada medida de

	seguridad que se aplique los delincuentes desarrollan otro medio de interceptar la información personal de la persona que ellos deseen robar sus datos y hacer mal uso de ello.
CHUPILLÓN (2023)	Las medidas de seguridad de hoy en día no son muy conocidas por la sociedad, por lo que aún siguen exponiendo sus datos sin tener cuidado, esto sucede por la falta de conocimiento. Hay muchas personas que solo usan las redes sociales para conocer más personas exponiendo toda su información sin impórtales con quien las comparte.
CHUQUIRUNA (2023)	Las medidas de seguridad que existen limitan la interceptación de datos informáticos y protegen la privacidad y la integridad de la información, por lo que han demostrado ser efectivas para dificultar la interceptación no autorizada de datos informáticos.
IKEHARA (2023)	El Dr. Da una opinión afirmativa, pero también indica que estas medidas son transitorias, ya que con el avance de la tecnología se genera nuevas formas de criminalidad y dificulta que las medidas limiten del todo la interceptación de datos informáticos.
VASQUEZ (2023)	Para el Dr. No basta con las medidas que hay, sino también depende de cada sujeto quien se encarga de implementar las medidas de seguridad que se apliquen mejor a su actividad en específico.

LLUEN (2023)	En opinión de la dra. Indica que no limitan del todo el acto delictivo, porque los mismos delincuentes conocen de tecnología, conforme la tecnología evoluciona los delincuentes también lo hacen y conocen mil maneras de realizar el acto delictivo.
JUAREZ (2023)	Ella menciona que no limitan del todo, por ende, no hay disminución del delito, además de que al realizar este delito lo hacen con el único fin de obtener beneficios económicos, sin impórtales el daño que causan a sus víctimas.

Fuente: Elaboración propia

Objetivo Específico 1: Determinar las medidas de seguridad adoptadas por la regulación peruana en la interceptación de datos informáticos.

A continuación, se muestra una tabla, la cual contiene el nombre del entrevistado y su respuesta:

Tabla 5

ENTREVISTADO	RESPUESTA
TOLENTINO (2022)	Una de las medidas de seguridad más conocidas y que todos lo pueden usar sin problema es la de tener un antivirus actualizado, ya que este es un método para evitar los ataques informáticos, muchas veces por medio de un virus es que acceden a nuestros datos personales. Otra manera es la de tener un software también actualizado, este instrumento nos

	permite realizar distintas tareas en una computadora y si logran tener acceso a este software pone en peligro toda la información personal que podamos tener en una computadora.
CHUPILLÓN (2023)	Las medidas de seguridad que se usan en el Perú las más conocidas o comunes es tener una contraseña segura, proteger el correo electrónico, la cual es usada por todo el mundo y para su creación brindan información personal y al tener una contraseña segura protegen que sean hackeados por personas que quieran hacerle daño, muchas veces estas medidas no son aplicadas correctamente por la sociedad, de tal manera que dejan vulnerables a que cualquiera pueda usar su información personal con fines de lucro.
CHUQUIRUNA (2023)	Se ha suscrito un importante convenio en el ámbito de la ciberdelincuencia, esto es el convenio de Budapest, que ha tenido como objetivo servir como un marco normativo internacional para abordar y combatir los nuevos delitos relacionados con el internet.
IKEHARA (2023)	No se tiene, desde mi punto de vista, una regulación de mecanismos de prevención; y, me parece bien, pues, si fuese así se tendría la necesidad de estar modificando la ley de manera continua a causa de los avances tecnológicos.

VASQUEZ (2023)	Para el Dr. Las medidas de seguridad no se encuentran reguladas de forma expresa en la legislación nacional de forma imperativa. Cada sujeto u organización deberá determinar qué medida de seguridad o de mitigación de riesgo se acopla a su actividad.
LLUEN (2023)	En mi opinión La medida de seguridad que se ha tomado es la creación de una ley para prevenir y sancionar todos los delitos que se comentan al realizar la interceptación de datos informáticos, la ley es el N° 30096, la cual se encarga de dar las sanciones de acuerdo a la gravedad del delito.
JUAREZ (2023)	En mi opinión, se crea la ley N° 30096 (Ley de Delitos Informáticos) con el único objetivo de prevenir y sancionar los delitos cometidos por medio de la interceptación de datos informáticos.

Fuente: Elaboración propia

Objetivo Específico 2: Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

A continuación, se muestra una tabla, la cual contiene el nombre del entrevistado y su respuesta:

Tabla 6

ENTREVISTADO	**RESPUESTA**

TOLENTINO (2022)	Este delito es la raíz para que se produzcan otros más, tenemos la pornografía infantil, no solo con la interceptación de datos causa daño a los adultos, sino también a los menores de edad ya que estos son los que están más expuestos y comparten su información sin tomar medidas de seguridad, basta con que intercepten una foto de la menor para publicarla en los sitios de pornografía, claro que estas fotos son publicadas sin autorización de la menor o de sus padres, esto lo realizan con el único fin de obtener dinero
CHUPILLÓN (2023)	Depende de la gravedad del delito, la interceptación de datos informáticos causa otros delitos como al patrimonio, fraude, robo, etc., para que se determine la sanción o pena se evalúa el daño que causo o que produjo por la interceptación de datos informáticos. Las penas establecidas se encuentran en la ley N° 30096, por ejemplo, tenemos que la pena será no menor de 3 ni mayor de 5 años cuando se realice el tráfico ilegal de datos.
CHUQUIRUNA (2023)	Es un tema que depende de varios factores y puede ser motivo de debate, pero algunos delitos que se cometen por la interceptación de datos informáticos no son severos por lo que continúa cometiendo él delito.
	En opinión del Dr. Indica que las sanciones que se dan por la legislación peruana a los delincuentes que cometen el

IKEHARA (2023)	delito de interceptación de datos informáticos se podría decir que dentro de todo son proporcionales al acto delictivo.
VASQUEZ (2023)	La legislación penal de delitos informáticos regula sanciones penales a personas naturales, las cuales en mi opinión creo que son las adecuadas en la interceptación de datos informáticos, ya si se comete otros delitos por medio de este creo que debería ser más severo.
LLUEN (2023)	La dra. Tiene una respuesta positiva, pero cree que puede mejorarse para acelerar las investigaciones y encontrar al delincuente, esto muchas veces toma tiempo ya que se debe descifrar códigos, etc., las sanciones que se encuentran a mi criterio son muy leves, por lo que no disminuye este delito, debería ser más severos.
JUAREZ (2023)	A pesar de las sanciones que se encuentran tipificadas en la ley N° 30096, se siguen cometiendo y no disminuye el delito, en lo personal creo que se debe a que las sanciones con las que se les castiga son muy leves para los delincuentes por lo que no sienten temor a ser castigados y siguen cometiendo una y otra vez el mismo delito.

Fuente: Elaboración propia

Como se pudo apreciar cada entrevistado tiene su punto de vista, algunos concuerdan en algunos puntos mientras que otros están en desacuerdo. Pero la mayor parte cree que las

sanciones que se dan para este delito deberían ser más severo, ya que este delito permite en ocasiones que se produzcan otros delitos más graves, teniendo como víctimas no solo a las personas adultas, sino también a menores de edad.

Para llegar a estas respuestas por parte de los entrevistados, las preguntas que se realizaron fueron las siguientes:

Tabla 7

OBJETIVOS	PREGUNTAS
OBJETIVO GENERAL	Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos?
	Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles?
	Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué?
	¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo?
	¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos?

OBJETIVO ESPECÍFICO 1	Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué?
	Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?
OBJETIVO ESPECÍFICO 2	En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué?
	¿Cree que se puede mejorar estas sanciones? ¿Cómo?
	¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos?

Fuente: Elaboración propia

Asimismo, se realizó el análisis de la Ley N° 30096 (Ley de Delitos Informáticos):

La Ley N° 30096, ley de delitos informáticos se publicó y entro en vigencia el 22 de octubre de 2013, esta ley tiene como objetivo sancionar y prevenir las conductas ilícitas que afecten los datos informáticos y que por medio de ello se de otros delitos, la cual se da por medio del uso de la tecnología de la información o de la comunicación.

La ley mencionada se crea con el fin de garantizar la lucha contra la interceptación de datos informáticos, además de que en nuestro código penal no se encuentra tipificado ningún artículo que haga mención las sanciones cometidas por este delito.

Esta ley tiene sanciones para los delitos que se producen a raíz de la interceptación de datos informáticos, tenemos el delito contra el patrimonio, delitos contra datos y sistemas informáticos, delitos informáticos contra la indemnidad y libertad sexual, contra intimidad y el secreto de comunicaciones, así como estas hay otros delitos que se encuentran en esta ley, pero en realidad esto hace disminuir la interceptación de datos informáticos. Ha análisis propio no lo hace.

Según Ávalos (2020) en el artículo "*Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada*", en nuestro país las cifras del Ministerio Público evidencian que las denuncias por delitos informáticos se incrementan año tras año. Esto nos indica que a pesar que existe una ley que sanciona el delito, este sigue en aumento, es decir en vez de disminuir está en crecimiento, esto no se debe solo a las medidas que se aplican, sino que la sociedad no tiene cuidado con quien comparte su información personal, no se protegen al ingresar a páginas que no conocen o al abrir archivos que le pueden llegar con virus.

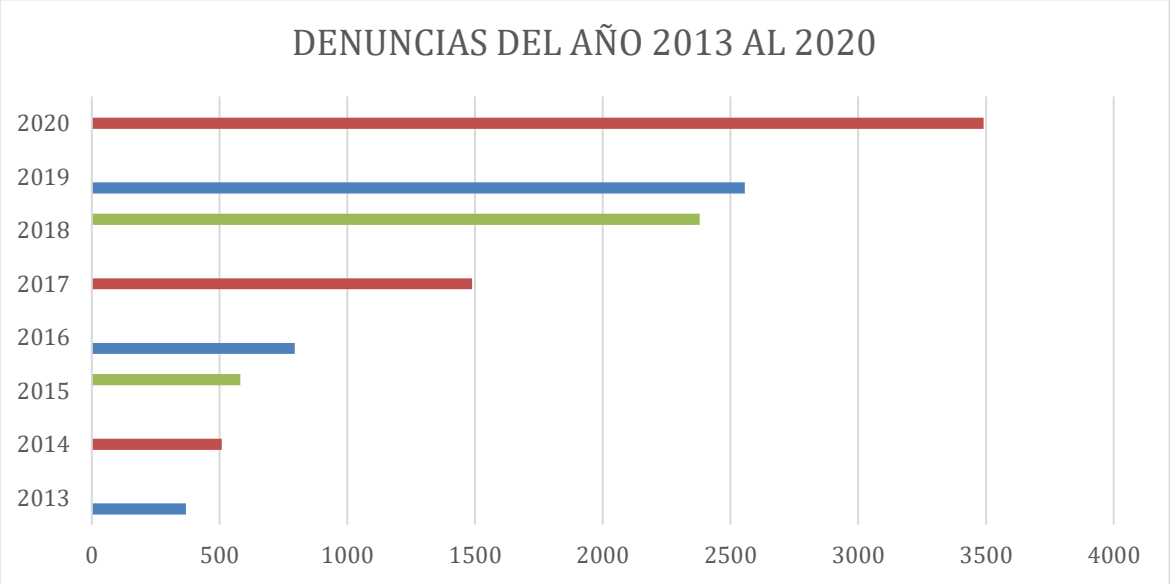
La autora mencionada anteriormente también nos indica que entre 2013 y 2020, tanto como en las fiscalías penales y mixtas registraron 21,687 denuncias de las cuales el 40% pertenece solo al 2019, es demasiado las denuncias que se registran, es obvio que se puede apreciar que aún se sigue con la lucha contra el delito de interceptación de datos informáticos y que a pesar de la ley que los sanciona no basta para que se detengan o disminuyan.

La ley sanciona de manera leve, es decir que no causa temor a los delincuentes que cometen este delito, al no tener temor es que se encuentra en aumento dicho delito que no solo perjudica a las personas sino también al estado. Para que esto no suceda se debe brindar una capacitación constante de la manera correcta del uso de las medidas de seguridad que existe en el Perú, esta capacitación debe ser llevada también en los colegios, ya que los

menores son los que corren más riesgo con este delito, son ellos los que comparten su información sin temor a las consecuencias, como no conocen el daño que les puede causar hasta que les afecte, continúan compartiendo su información.

A continuación, se elabora un gráfico para mostrar el aumento que se dio en los últimos años, los datos utilizados fueron obtenidos del Ministerio Público de su informe titulado: “Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada”.

Figura 3



Fuente: Elaboración propia con información del ministerio publico

Como se aprecia en esta imagen que con el pasar de los años el delito de interceptación de datos informáticos ha ido en aumento, no existe ninguna disminución del delito, que nos da a entender esto, que las sanciones que se da para este delito por nuestra legislación no es severa o no es lo suficiente para que disminuya, no solo esta las sanciones, sino que la sociedad no conoce sobre las medidas de seguridad que existen para proteger la información privada de cada uno.

CAPÍTULO IV: DICUSIÓN Y CONCLUSIONES

4.1 Discusión

En este extremo de la investigación se podrá identificar y analizar las limitaciones que hubo en función a la hipótesis planteada. Así como también hubo dificultades para obtener las entrevistas.

Uno de los factores con lo que se tuvo que lidiar fue la falta de tiempo por parte de los entrevistados, el internet, así como la búsqueda de las personas que se entrevistaría para obtener resultados sobre el tema de investigación, la cual no se pudo obtener la cantidad que se esperaba.

Para obtener información sobre el tema se realizó una búsqueda entre el periodo 2015-2023 con el fin de obtener información actualizada de los últimos años. De esta búsqueda encontramos 12 artículos empíricos, de los cuales se hablan sobre la seguridad informática, delitos informáticos, población y muestra, y los métodos científicos que se usan para la investigación.

Estos criterios son importantes en el trabajo investigado, ya que con esto se puede conocer sobre el tema, asimismo tener en cuenta que existen medidas de seguridad que se pueden usar o aplicar para poder proteger nuestra información personal y así evitar la interceptación de datos informáticos en nuestra sociedad.

Es necesario proteger y salvaguardar la información personal con la finalidad de evitar que un atacante pueda suplantar su identidad, (Barrantes, Sánchez, & Gutiérraz, 2020). Este autor habla sobre que depende de cada uno proteger nuestros datos para evitar la suplantación de identidad en un futuro. Además de que depende de nosotros proteger nuestra información y tener cuidado con quien compartimos estos datos personales.

Fuera de los artículos empíricos que se usó para dar apoyo a la investigación, también analizamos la Ley N° 30096, la cual no solo sanciona la interceptación de datos informáticos, este delito ocasiona otros en los cuales también se involucran a menores de edad, al patrimonio, trata de personas, entre otros. A pesar de las sanciones que se dan, aún continúa en marcha este delito, sin ver disminución alguna, es decir que las penas o sanciones puestas en la ley mencionada no son suficientes para combatir este delito. Por lo que se debería considerar unas penas mayores dependiendo el grado del delito.

Asimismo, se realizaron entrevistas las cuales nos sirvieron para dar respuesta a nuestros objetivos,

En las entrevistas que se realizaron se pudo concluir en el objetivo general la cual trata de "Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana en el 2021-20122"que los entrevistados consideraban que no todos conocen las medidas de seguridad que existen para cuidar nuestros datos informáticos,, así como también de que las sanciones brindadas por nuestra regulación peruana no es la adecuada, ya que no se ve disminución en el delito de interceptación de datos. Es decir que mayormente las personas que conocen sobre el tema son aquellas que fueron victimas o profesionales relacionados al tema.

Para el objetivo específico 1 que es "Determinar las medidas de seguridad adoptadas por la regulación peruana en la interceptación de datos informáticos" hicieron mención de algunas medidas que ellos creían que eran las más comunes y usadas por la mayoría de la sociedad, en estas tenemos un antivirus, la cual protege al usuario de los virus que se les pueda mandar de manera camuflada, ya sea mediante un correo, invitación, formulario entre otros, otra es de usar una contraseña que no sea muy obvia, es decir de que muchas veces se

usa como contraseña las fechas de cumpleaños, apellidos, nombre de la novia (o), entre otros, lo correcto sería usar una que nadie pueda deducirlo rápidamente.

Por último, para el objetivo específico 2 que es "Determinar las sanciones adoptadas por la regulación peruana para el delito de interceptación de datos informáticos", en este objetivo los entrevistados están de acuerdo en que el delito de interceptación de datos informáticos produce u ocasiona delitos con más gravedad. Ellos creen que la sanción que se da en nuestra regulación peruana no es lo sufrientemente severa, ya que no se puede observar ninguna disminución del delito.

No solo las personas naturales pueden ser víctimas del delito de interceptación de datos sino también personas jurídicas como se menciona en el expediente de habeas corpus en la cual se ven involucradas personas jurídicas, es decir empresas que poseen información muy valiosa que al ser interceptadas pueden ocasionarles un daño irreparable.

Solo las personas u organizaciones ponen en peligro su información a causa de la mínima seguridad que implementan, sino también por el poco conocimiento del uso adecuado de la información o de las herramientas que existen para proteger nuestros datos personales en el internet, (León & Toscano, 2020). Muchas veces las empresas jurídicas ponen en riesgo su información por no conocer o implementar las medidas de seguridad adecuadas para la protección de su información.

Es claro que todos están expuestos a la interceptación de datos informáticos, ya sean personas naturales o jurídicas, esto sucede por el simple hecho de no conocer la manera adecuada o de tener cuidado con nuestra información personal.

4.2 Recomendación

Es claro que nadie se salva del delito de interceptación de datos informáticos, por lo que se recomienda que el Estado de charla en los colegios, comunidades, etc., a padres de familia, estudiantes, a personas de tercera edad, sobre el delito mencionado con el fin de evitar que se sigan cometiendo este delito.

También se pueden brindar cursos gratuitos sobre el uso adecuado del internet, de lo que se puede o no compartir en redes sociales, usar adecuadamente los medios de protección que existen para proteger nuestra información.

4.3 Conclusión

Los documentos como entrevistas y análisis documental fueron recolectados para poder tener apoyo en el presente trabajo, esto con el único fin de que todos conozcan o sepan de los problemas que ocasiona el avance de la tecnología si no se tiene cuidado en su uso diario.

Además de que este tema ocasiona o es la base para que se produzcan otros delitos, muchos de ellos son graves que hasta involucran a menores de edad, la cual puede marcar de por vida a las víctimas

También podemos concluir que las sanciones que se dan en la ley N°30096 no están surgiendo efecto en la disminución del delito de interceptación de datos, esto quizás se da por que las sanciones que se realizan ante un delito no son suficientes para que este disminuya.

Además, que de acuerdo a las entrevistas se puede concluir que se debe usar de manera responsable las redes sociales, al momento de llenar formularios, entre otros, no se debe compartir la información personal con cualquiera y peor aún si es un desconocido,

siempre se debe usar algún tipo de medida de seguridad que pueda ayudar a proteger lo más valioso de cada persona, es decir su información para que luego no se vean perjudicados en el futuro.

REFERENCIAS

- Alvarado, F. (2016). *La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales*. Revista, Lima: PUCP http://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19833/19877
- Nevárez, A. (2017). *Robo de información, más común de lo que creen*. Revista ResearchGate https://www.researchgate.net/profile/Alberto_Quintana-Nevarez/publication/314772203_Robo_de_informacion_mas_comun_de_lo_que_todos_creen/links/58c5e88fa6fdcce648e8b804/Robo-de-informacion-mas-comun-de-lo-que-todos-creen.pdf
- Romero, M. (2017). *Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016.* Revista: Universidad de Huánuco-Huánuco. http://repositorio.udh.edu.pe/bitstream/handle/123456789/331/T_047_%2025858529_T.pdf?sequence=1&isAllowed=y
- Zenabria, E.; Cayo, E. (2018). *Seguridad informática en dispositivos móviles con sistemas operativos android mediante pentesting*. Revista: Universidad Nacional del Altiplno-Puno http://repositorio.unap.edu.pe/handle/UNAP/7047
- Valladolid, N; Chávez, M. (2020) *El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis*. Artículo para la revista Vox Juris, ISSN 1812-6804, Vol. 38, N°**2** https://dialnet.unirioja.es/servlet/articulo?codigo=7628480
- Cotán, A. (2016). *El estudio de la investigación cualitativa*. Artículo para Escuela

Abierta, 19:33-48 ISSN: 1138-6908, Consultado en: 10 de julio de 2020. https://dialnet.unirioja.es/descarga/articulo/5815704.pdf

- Otero, A. (2018). *Enfoques de Investigación*. Artículo de Google académico https://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf
- Hernández, J; Herrera, L; Martínez, R; Páez, J; Páez, M. (2011). Artículo de la revista Academia Accelerating the world's research. https://d1wqtxts1xzle7.cloudfront.net/42814536/INFORME-TEORIA-FUNDAMENTADA-with-cover-page v2.pdf?Expires=1625876795&Signature=GGxQzRiUpCNex1XnRl6PfqoZR-1pQnI7nZXWREyG2YY31LgepjpC49ifq28g3MlkX8cexwpPCngh9LlP38x0hbHjg WmtFQFK4j7TK1dRs3FEN8MdCrru1HsVva09Bok8SgxMG0MS6X8c91i9A3Yr1 QZTzo0xWL6faU0YKGR64MQHd9OD8IzYFTvtnIG8JqFTbsY7kx-9mwW-iF9Q2ds9QagvKE-VtS6hDP7k3p-9XPNXzGTGT2gddMpU-8mzrQoYPxmRMJ1KN5pSLpXNF 7rT1zPryQ4JlhaFVsRqbIEv0qx8cVjrhKNVVTrQ-Kf2t~E1xSywVNArU-8IHQqoBneOA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- Martínez, P. (2006). *El método de estudio de caso: estrategia metodológica de la investigación científica*. Revista Pensamiento & Gestión 20:165-193, ISSN: 1657-6276 https://www.redalyc.org/pdf/646/64602005.pdf
- Toledo, N. (2016). *Población y Muestra*. Revista: Material didáctico: solo visión-Lima

http://ri.uaemex.mx/bitstream/handle/20.500.11799/63099/secme26877.pdf?sequence=1

- Castillo, L. (2015) *Biblioteconomía - Segundo Cuatrimestre, Análisis documental*. Consultado en: 4 de julio 2020 https://www.uv.es/macas/T5.pdf
- Palmet, A. (2020) *Petroglifos*. Revista Crítica Transdisciplinaria ISSN: 2610-8186 https://petroglifosrevistacritica.org.ve/revista/metodos-inductivo-deductivo-y-teoria-de-la-pedagogia-critica/
- Ávalos, Z. (2020). *Ciberdelincuencia: Pautas para una investigación fiscal especializada.* Revista: Ministerio Público-Lima https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf
- Barrantes, J.; Sanchez, J.; Gutierrez, S. (2020). *Seguridad de la información ¿Cómo proteger los datos personales?* https://repositorio.ins.gob.pe/handle/INS/1185
- León, O.; Toscano, G. (2020). *Propuesta de evaluación del tratamiento de los datos personales para medir el nivel de cumplimiento de la Ley N° 29733 en Jadal Software S.A.C.* Repositorio: UTP https://repositorio.utp.edu.pe/handle/20.500.12867/3895
- Ocampo, Meylin del Pilar Romero (2017), Delitos informáticos cometidos a través de redes sociales y su tratamiento en el ministerio público en la ciudad de Huánuco, 2016. Repositorio universitario de la universidad de Huánuco (pag.10-11)

ANEXOS

ANEXO N° 1: Matriz de viabilidad.

PROBLEMA	OBJETIVO	HIPÓTESIS	METODOLOGÍA
Problema general ¿De qué manera las medidas de seguridad limitan interceptación de datos informáticos en la regulación peruana en el periodo 2021-2022? **Problemas específicos** _ ¿Cuáles son las medidas de seguridad adoptadas por la regulación peruana en la interceptación de datos informáticos? _ ¿Cuáles son las sanciones adoptadas por la regulación peruana para el delito de interceptación de datos informáticos?	**Objetivo general** Determinar de qué manera las medidas de seguridad limita la interceptación de datos informáticos por la regulación peruana en el periodo 2021-2022. **Objetivos específicos** _ Determinar las medidas de seguridad adoptadas por la regulación peruana en la interceptación de datos informáticos. _Determinar las sanciones adoptadas por la regulación peruana para el delito de interceptación de datos informáticos.	**Hipótesis general** Las medidas de seguridad limitan a la interceptación de datos informáticos al momento de que la sociedad comparte información personal. **Hipótesis específicas** _Las medidas de seguridad adoptadas por la regulación peruana ayudan a la sociedad a mantener a salvo los datos personales que comparten diariamente. _Las sanciones adoptadas por la regulación peruana se encuentran tipificadas en la ley N° 30096 en la que se observa que por medio de este delito se ocasionan otros delitos que perjudica a la sociedad.	**Enfoque de Investigación** Cualitativo **Tipo de Investigación** Básico, no experimental **Diseño de la Investigación** Teoría fundamentada **Instrumentos** Guía de análisis documental y entrevista **Población y muestra** Análisis de ley y entrevistas (7)

ANEXO N° 2: Guía de Validación por expertos

GUIA DE EVALUACION DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: FERNANDO IKEHARA VELIZ

TÍTULO Y GRADO: Abogado y Magister en Derecho Penal

Doctor ( ) magister (X) licenciado ( )

Otros: (Especifique): Ninguno

INSTITUCION Y ESPECIALIDAD QUE LABORA: Pazos Ikehara Abogados, Universidad Privada del Norte y Universidad Científica del Sur

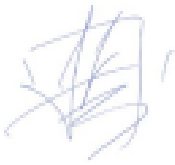
FECHA: 18/10/2023

TITULO DE LA INVESTIGACIÓN: "MEDIDAS DE SEGURIDAD Y LA INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN LA LEGISLACION PERUANA 2021 - 2022"

Mediante la tabla de evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicar sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia en las preguntas.

N°	PREGUNTAS	APRECIA		OBSERVACIONES
		SI	NO	
1	¿El título de la investigación tiene relación con el instrumento de recolección de datos?	Si		Ninguno
2	¿Las variables de estudio se relacionan con el instrumento de recolección de datos?	Si		Ninguno
3	¿El instrumento de recolección de datos, responde a los objetivos del estudio?	Si		Ninguno
4	¿Cada una de las preguntas del instrumento de medición,	Si		Ninguno

	se relaciona con cada uno de los elementos de los indicadores?			
5	¿La redacción de las preguntas tienen coherencia	Si		Ninguno
6	¿El instrumento de medición es claro, preciso y sencillo para que contesten y de esta manera tener los datos requeridos?	Si		Ninguno
7	¿El instrumento de recolección de datos contribuirá el análisis y procesamiento de datos?	Si		Ninguno
	TOTAL	7		

FIRMA	SELLO
	

ANEXO N° 3: Guía de validación por expertos

GUIA DE EVALUACION DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Michael Lincold Trujillo Pajuelo

TÍTULO Y GRADO:

Doctor ( ) magister (x) licenciado ( )

Otros: (Especifique):

INSTITUCION Y ESPECIALIDAD QUE LABORA:

FECHA:

TITULO DE LA INVESTIGACIÓN: "MEDIDAS DE SEGURIDAD Y LA INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN LA LEGISLACION PERUANA 2021 - 2022"

Mediante la tabla de evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicar sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia en las preguntas.

N°	PREGUNTAS	APRECIA		OBSERVACIONES
		SI	NO	
1	¿El título de la investigación tiene relación con el instrumento de recolección de datos?	x		
2	¿Las variables de estudio se relacionan con el instrumento de recolección de datos?	x		
3	¿El instrumento de recolección de datos, responde a los objetivos del estudio?	x		
4	¿Cada una de las preguntas del instrumento de medición, se relaciona con cada uno de	x		

	los elementos de los indicadores?			
5	¿La redacción de las preguntas tienen coherencia	x		
6	¿El instrumento de medición es claro, preciso y sencillo para que contesten y de esta manera tener los datos requeridos?	x		
7	¿El instrumento de recolección de datos contribuirá el análisis y procesamiento de datos?	x		
	TOTAL	7		

FIRMA	SELLO
	C.A.L 54649 Michael L. Trujillo Pajuelo

ANEXO N° 4: Guía de validación por expertos

GUIA DE EVALUACION DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: JOSE ARTURO MATOS MONCADA

TÍTULO Y GRADO:

Doctor ( ) magister (X) licenciado ( )

Otros: (Especifique):

INSTITUCION Y ESPECIALIDAD QUE LABORA:

ABOGADO ESPECIALISTA EN LITIGIOS PENALES Y SOCIO FUNDADOR DE LA FIRMA LEGAL MATOS & ASOCIADOS.

FECHA: 17 de octubre del 2023.

TITULO DE LA INVESTIGACIÓN: "MEDIDAS DE SEGURIDAD Y LA INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN LA LEGISLACION PERUANA 2021 - 2022"

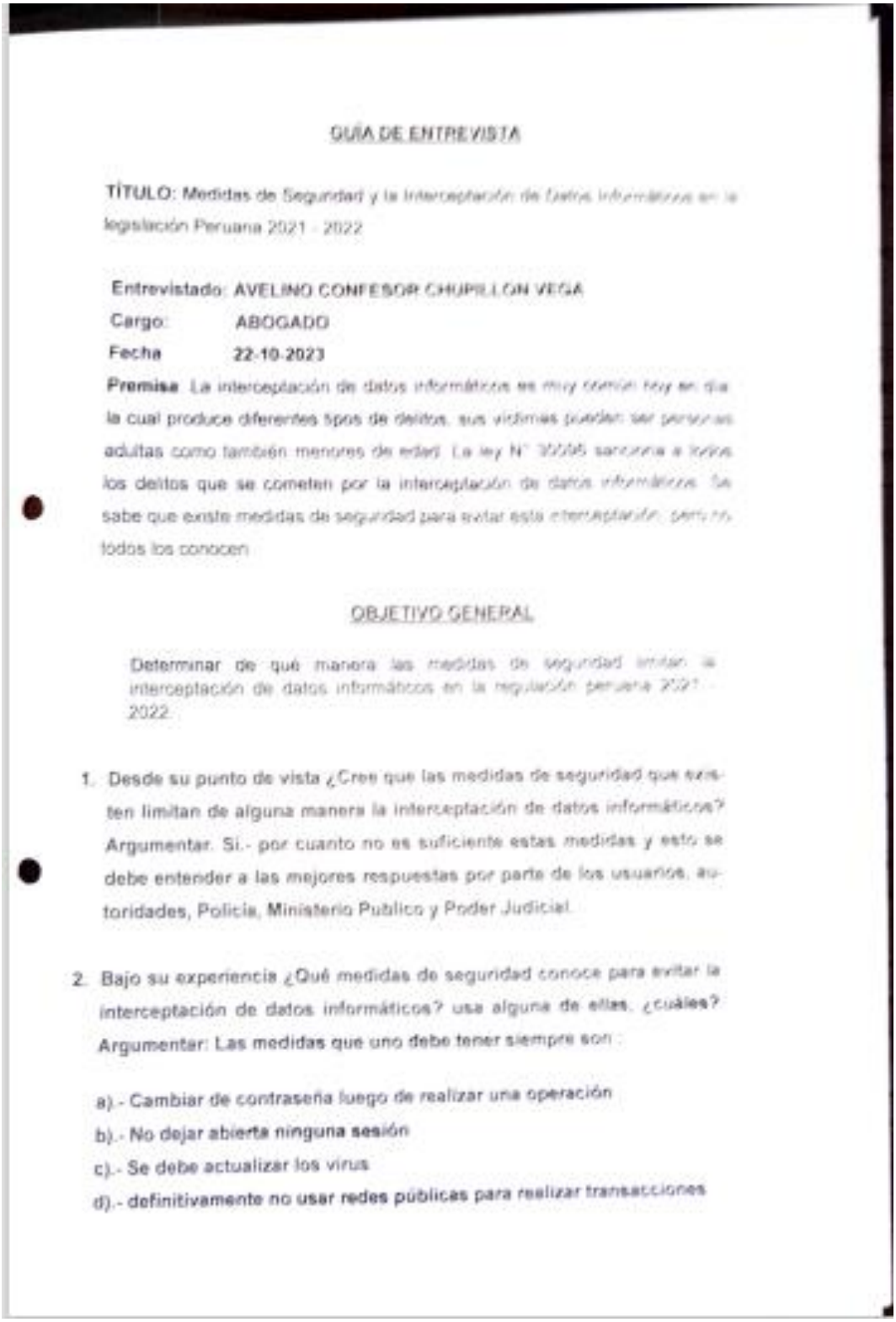
Mediante la tabla de evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicar sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia en las preguntas.

N°	PREGUNTAS	APRECIA		OBSERVACIONES
		SI	NO	
1	¿El título de la investigación tiene relación con el instrumento de recolección de datos?	Si		
2	¿Las variables de estudio se relacionan con el instrumento de recolección de datos?	Si		
3	¿El instrumento de recolección de datos,	Si		

	responde a los objetivos del estudio?			
4	¿Cada una de las preguntas del instrumento de medición, se relaciona con cada uno de los elementos de los indicadores?	Si		
5	¿La redacción de las preguntas tienen coherencia	Si		
6	¿El instrumento de medición es claro, preciso y sencillo para que contesten y de esta manera tener los datos requeridos?	Si		
7	¿El instrumento de recolección de datos contribuirá el análisis y procesamiento de datos?	Si		
	TOTAL	7		

FIRMA	SELLO
	

ANEXO N° 5: Guía de entrevista a Avelino Confesor Chupillón Vega



GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la legislación Peruana 2021 - 2022

Entrevistado: AVELINO CONFESOR CHUPILLON VEGA
Cargo: ABOGADO
Fecha 22-10-2023

Premisa La interceptación de datos informáticos es muy común hoy en día la cual produce diferentes tipos de delitos, sus víctimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos? Argumentar. Si.- por cuanto no es suficiente estas medidas y esto se debe entender a las mejores respuestas por parte de los usuarios, autoridades, Policía, Ministerio Público y Poder Judicial.

2. Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar: Las medidas que uno debe tener siempre son :

   a).- Cambiar de contraseña luego de realizar una operación
   b).- No dejar abierta ninguna sesión
   c).- Se debe actualizar los virus
   d).- definitivamente no usar redes públicas para realizar transacciones

3. Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar: No, No son las adecuadas; sin embargo se debe concientizar a los usuarios y sociedad en general a fin de que tengan cuidado al momento de aperturar alguna cuenta bancaria u otros.

4. ¿Por qué cree Ud. que se siguen cometiendo el delito de intercepta ción de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar,- Se siguen cometiendo esta clase de delitos por falta de formación, información y orientación a los usuarios y a las autoridades.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. ¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar,- Las medidas de seguridad, son la de prevenir y sancionar las comisiones ilícitas en cuanto a este delito, y otras seria: La formación, información y orientación a los usuarios y a las autoridades.

6. Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar: No son las correctas, pero se tendría que mejorar, informando y orientando al usuario y capacitando a las autoridades en cuanto a a esta tecnología.

7. Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?,- Seria de la de prevención por parte del usuario y la oportuna orientación al usuario y la debida seguridad por parte de las entidades crediticias en que tienen ahorrado su cartera de clientes y de las empresas para realizar la operación de cualquier bien mueble e inmueble.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos

8. En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar; No.-Porque como reitero es insuficiente, debido a que las sanciones o penas no dan solución, lo que se debe es concientizar a la ciudadanía y a nuestras autoridades encargadas de hacer cumplir la ley.

9. ¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar; Si mediante un estudio tecnificado.

10. ¿Qué se debería hacer para que se disminuya el delito de intercepta-ción de datos informáticos? Argumentar.- La debida orientación al usuario, entidades crediticias y empresas, en manejo de equipos informáticos.

FIRMA	SELLO
	Abelardo C. Chupillón Vega ABOGADO C.A.L. N° 23629

ANEXO N° 6: Guía de entrevista a Delia Yenny Juárez Neyra

GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la legislación Peruana 2021 - 2022.

Entrevistado : **Delia Yeny Juarez Neyra**
Cargo : **Fiscal Adjunta Provincial de la Octava Fiscalia Provincial Penal corporativa del Callao.**
Fecha : **17 de octubre de 2023.**

Premisa: La interceptación de datos informáticos es muy común hoy en día, la cual produce diferentes tipos de delitos, sus víctimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen.

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. **Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos? Argumentar.**

   Las medidas de seguridad no limitan del todo la interceptación de datos, es decir que no disminuye este delito, con el pasar del tiempo evoluciona la tecnología y con ello también las personas que cometen este delito, ellos lo hacen con el único fin de obtener ganancias económicas para sí mismas sin importarle a quien lastime en el proceso. Es de suma importancia que cada uno proteja su información y no la comparta con desconocidos, ya que no solo depende de las medidas de seguridad que se apliquen por cada persona, sino también de uno mismo si no quiere salir perjudicado por el simple hecho de distribuir su información.

2. **Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar:**
   Las más común es usar una contraseña, antivirus actualizado, las que uso son las que se mencionó anteriormente además de usar la nube, en la cual guardo información importante y se crea una copia de seguridad para recuperar por si pasa algo con la nube

3. **Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar.**
   No, porque aun se siguen cometiendo el delito de interceptación de datos informáticos, a mi parecer las sanciones son muy leves, a causa de este delito se comenten otros en las cuales muchas veces están involucrados menores de edad, para las cuales el castigo debería ser severo. Al cometer este delito la pena privativa de libertad es no menor de 3 ni mayor a 6 años. Creo que es muy leve por lo que aun no disminuye el delito mencionad anteriormente.

4. **¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar.**
   Este delito continuo por el simple hecho de que la legislación peruana no es severa, si nuestro país fuera mas estricta en ciertos aspectos este delito disminuiría, quizás no desaparezca, pero si disminuya.
   Informar a la sociedad del peligro que corren al compartir su información personal, también ser mas estrictos con las sanciones. Además de informar todas las medidas de seguridad que existen y pueden usar para proteger su información de los hackers, de esta manera se evita ser victima de los delincuentes informáticos.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. **¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar**

   La legislación peruana por proteger nuestra información personal creo la ley N° 30096 (Ley de Delitos Informáticos) con el único objetivo de prevenir y sancionar los delitos cometidos por medio de la interceptación de datos informáticos.

6. **Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar:**

   Esta medida tomada por la legislación peruana es la correcta, pero no del todo, ya que el delito se sigue cometiendo y las victimas no solo son personas adultas, empresas, sino también involucran a menores edad.

7. **Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?**

   Creo que hacer conocida a la ley 30096, no toda la sociedad sabe sobre esta ley, a mi parecer los que conocen del tema son los que por alguna razón han tenido que ver en sus estudios con leyes.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

8. **En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar**

   No, porque a pesar de las sanciones que se encuentran tipificadas en la ley N° 30096, se siguen cometiendo y no disminuye el delito, en lo personal creo que se debe a que las sanciones con las que se les castiga son muy leves para los delincuentes por lo que no sienten temor a ser castigados por lo que lo siguen cometiendo.

9. **¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar**

Claro que si, la cuestión es que tanto el pueblo como los que nos representan estén de acuerdo en poner leyes mas severas para este tipo de delitos, y de ser el caso agilizar en los procesos y que no se estanquen en las investigaciones.

10. **¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos? Argumentar**

Ser cuidadosos con lo que cada uno publica y comparte en las redes sociales sobre su información personal, para así no ser víctimas de delincuentes cibernautas

FIRMA	SELLO
	Delia Yenny Juarez Neyra Fiscal Adjunta Provincial Fiscalía Provincial Penal Corporativa

ANEXO N° 7: Guía de entrevista a Claudia Lluen Espino

GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la legislación Peruana 2021 - 2022.

Entrevistado : Claudia Lluen Espino
Cargo : Fiscal adjunta Provincial de la Primera Fiscalía Provincial Penal Corporativa del Distrito Fiscal del Callao
Fecha : 15/10/2023

Premisa: La interceptación de datos informáticos es muy común hoy en día, la cual produce diferentes tipos de delitos, sus víctimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen.

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. **Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos? Argumentar.**
   No del todo, quizás por que los mismos delincuentes conocen del tema y no tienen miedo, además que para ser castigados les toma tiempo en encontrar pruebas para confirmar la identidad del delincuente.

2. **Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar:**
   Las que conozco o las mas comunes son contar con una contraseña ya sea para el correo electrónico, o para ingresar muchas veces a alguna cuenta bancaria, también hay app que de alguna manera permiten que archivos importantes se copien y se guarden automáticamente por si ocurre algo con el

aparato que se usa para realizar trabajos, una de esta app sería el Drive y la Nube, las cuales también uso para guardar archivos importantes.

3. **Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar.**

   No del todo, porque podrían ser mas severas, muchas veces por medio de este delito las empresas pierden miles de dólares, las cuales no pueden ser recuperas, además de que las investigaciones toman su tiempo, por lo que se debería castigar de manera severa que el delincuente no quiera volver a cometer otra vez este delito.

4. **¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar.**

   Sigue existiendo por la falta de conocimiento de la sociedad, si nosotros conociéramos el peligro que se corre con compartir una información personal, creo que se tendría mas cuidado al momento de publicar en las redes sociales datos personales, hoy en día no solo los adultos lo publican, mayormente los que hacen actualizaciones de sus publicaciones son menores de edad o adolescentes y ellos son los más vulnerables.
   Quizás para disminuir este delito el gobierno debería dar charlas gratuitas sobre estos temas tanto a los adultos como adolescentes, podrían brindar charlas en los colegios, realizar encuestas para que sepan cuantos son los que publican su información personal y que tipos de publicaciones realizan.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. **¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar**

La medida de seguridad que se ha tomado es la creación de una ley para prevenir y sancionar todos los delitos que se comentan al realizar la interceptación de datos informáticos, la ley es el N° 30096, la cual se encarga de dar las sanciones de acuerdo a la gravedad del delito.

6. **Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar:**
   Si son las correctas, pero creo que se pudo ser mas estricto en las sanciones. Se debe tener en cuenta que este delito ocasiona otras mas en las cuales se involucran no solo a adultos sino también a menores de edad.

7. **Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?**
   Informar a la sociedad del peligro que corren al momento de compartir su información personal con gente que nunca ha visto, además de informar a la sociedad de la existenciña de la ley N°30096, quien se encarga de castigar a los delincuentes que cometen este delito, así como brindarles charlas tanto a personas mayores como a menores, para prevenirles de los riesgos que corren por hablar y compartir todo en las redes sociales sin contar con algún tipo de seguridad informática.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

8. **En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar**
   Si, pero creo que puede mejorarse para acelerar las investigaciones y encontrar al delincuente, esto muchas veces toma tiempo ya que se debe descifrar códigos, etc., las sanciones que se encuentran a mi criterio son muy leves, por lo que no disminuye este delito, debería ser mas severas.

9. **¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar**

Todo depende de como es nuestro gobierno, muchas veces que observan que algo no les va favorecer ponen excusas para no realizar cambios en las leyes, por ejemplo, si en la interceptación de datos informáticos se ve involucrado uno de nuestros representantes, las investigaciones se tratan de agilizar, pero si es un ciudadano las investigaciones toman tiempo.

10. ¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos? Argumentar

Cada ciudadano debe ser consciente de la información que comparte con personas desconocidas, no solo los adultos, sino también que cada padre de familia este cuidando lo que sus menores hijos publican en sus redes sociales, de esta manera se puede evitar ser victimas de estos delincuentes.

FIRMA	SELLO
	CLAUDIA LEGUIA PINO FISCAL ADJUNTA PROVINCIAL

ANEXO N° 8: Guía de entrevista a Liliam Patricia Chuquiruna Atencia

GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la Legislación Peruana 2021 - 2022.

Entrevistado : **Lilliam Patricia Chuquiruna Atencia**
Cargo : **Fiscal adjunta Provincial de la Decimo Primera Fiscalia Provincial Penal Corporativa del Callao – Cuarto Despacho.**
Fecha : **19/10/2023**

Premisa: La interceptación de datos informáticos es muy común hoy en día, la cual produce diferentes tipos de delitos, sus victimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen.

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. **Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos? Argumentar.**
   Desde mi punto de vista, las medidas de seguridad que existen limitan la interceptación de datos informáticos y protegen la privacidad y la integridad de la información, por lo que han demostrado ser efectivas para dificultar la interceptación no autorizada de datos informáticos.

2. **Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar:**
   Uso el firewalls que es un dispositivo o programa que controla el tráfico de red y puede bloquear conexiones no autorizadas y con ello protejo mi red y mis dispositivos; asimismo uso el VPN que cifra el tráfico de internet y oculta

la dirección IP del usuario, lo que dificulta que terceros intercepten también la información, cuando necesito una conexión segura en redes públicas o cuando deseo acceder a contenido restringido geográficamente; por otro lado existe también el cifrado de datos que consiste en convertir la información en un formato ilegible a menos que se tenga la clave del descifrado adecuado, lo utilizaba cuando enviaba información sensible a través de la web o al almacenar datos confidenciales en dispositivos.

3. **Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar.**

   Considero que no del todo debido a que su regulación es insuficiente o carece de especificidad, esto se debe, en parte a que el campo de la ciberdelincuencia evoluciona constantemente y los legisladores desconocen o a menudo tienen dificultades para mantenerse al día con las amenazas emergentes y las tecnologías cambiantes.

4. **¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar.**

   Si, una de las razones podría ser la motivación económica pues muchos delincuentes informáticos están motivados por la ganancia económica, ya sea a través del robo de información financiera. Una de las maneras para evitarlo es ser responsables de proteger nuestros propios dispositivos y datos utilizando contraseñas fuertes y evitando prácticas inseguras, incluso garantizar el cumplimiento de las leyes para disuadir a los delincuentes informáticos y llevarlos ante la justicia.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. **¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar**

   Se ha suscrito un importante convenio en el ámbito de la ciberdelincuencia, esto es el convenio de Budapest, que ha tenido como objetivo servir como un marco normativo internacional para abordar y combatir los nuevos delitos relacionados con el internet.

6. **Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar:**

   Falta una base legal sólida para la persecución de los delincuentes.
   Fomentar la cooperación entre países para abordar los delitos informáticos transfronterizos.

7. **Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?**

   Invertir en la investigación y desarrollo de tecnologías avanzadas de seguridad informática y en la mejora continua de herramientas de cifrado y autenticación puede ayudar a reducir la vulnerabilidad de los sistemas a la interceptación de datos.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

8. **En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar**

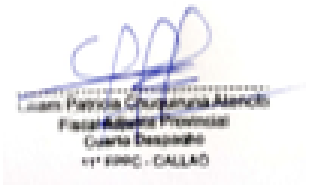
   Es un tema que depende de varios factores y puede ser motivo de debate, pero algunos delitos que se cometen por la interceptación de datos informáticos no son severos por lo que se continúa cometiendo él delito.

9. **¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar**

   Si creando leyes más severas que puedan incluir multas, prisión.

10. ¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos? Argumentar

Implementar tecnológicas avanzadas, como sistemas de inteligencia artificial para la detección de amenazas y podría ser la educación pública sobre la importancia de la seguridad informática, la privacidad en línea y la detección de intentos de interceptación de datos puede ayudar a prevenir estos delitos.

FIRMA	SELLO
	

ANEXO N° 9: Guía de entrevista a Renzo Jesús Vásquez Villacorta

GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la legislación Peruana 2021 - 2022.

Entrevistado : **RENZO JESUS VÁSQUEZ VILLACORTA**
Cargo : **ABOGADO PENALISTA - DOCENTE**
Fecha : **17 / 10 / 2023**

Premisa: La interceptación de datos informáticos es muy común hoy en día, la cual produce diferentes tipos de delitos, sus víctimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen.

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. **Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos? Argumentar.**

La ISO 27110 y demás modelos de prevención o Compliance de Ciberseguridad brindan medidas recomendaciones a los diferentes sujetos y entidades para salvaguardar la confidencialidad de sus datos, no obstante, cada sujeto deberá implementar las medidas de seguridad o mitigación de riesgo que se apliquen mejor a su actividad en específico.

2. **Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar:**

Se puede mencionar las siguientes:

- Protocolos de tratamiento de datos e información sensible al interno de la organización.
- Implementación de políticas de protección de datos personales.
- Utilización de software de encriptación de datos.
- Implementación de un programa de Compliance digital.

3. **Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar.**

La Ley de Delitos Informáticos es una ley penal que sanciona las conductas lesivas mediante el uso de medios informáticos o la vulneración de bienes jurídicos protegidos de naturaleza digital. Considero que muy aparte de las penas a las personas naturales existe un vacío referente a las sanciones especiales aplicables a las personas jurídicas que por negligencia o falta de control de riesgos generen delitos informáticos.

4. **¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar.**

Como toda conducta delictiva, la interceptación de datos nunca va a desaparecer, ya que la comisión del delito es parte de la conducta humana en sociedad, más aún en la actualidad cuando vivimos en una sociedad altamente tecnologizada. No obstante, se puede mitigar el riesgo de su comisión mediante una regulación más específica y profunda que regule a todos los actores de la conducta típica, y mediante el incentivo de implementación del Compliance digital y de ciberseguridad.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. **¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar**

Las medidas de seguridad no se encuentran reguladas de forma expresa en la legislación nacional de forma imperativa. Cada sujeto u organización deberá determinar que medida de seguridad o de mitigación de riesgo se acopla a su actividad.

6. **Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar:**

Cada sujeto u organización deberá determinar las medidas de seguridad o de mitigación de riesgos delictivos que sean mas adecuada a su actividad.

7. Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?

Cada sujeto u organización deberá determinar las medidas de seguridad o de mitigación de riesgos delictivos que sean más adecuada a su actividad.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

8. En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar

La legislación penal de delitos informáticos regula sanciones penales a personas naturales, si solo se habla del Quantum de pena no me parece que haya mayor debate.

9. ¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar

Si, implementando la responsabilidad penal de las personas jurídica por la comisión de delitos informáticos basado en la deficiente gestión de riesgos.

10. ¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos? Argumentar

Implementar medidas de prevención de ciberseguridad y Compliance digital.

FIRMA	SELLO
	

ANEXO N° 10: Guía de entrevista a Fernando Ikehara Véliz

GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la legislación Peruana 2021 - 2022.

Entrevistado : **Fernando Ikehara Véliz**
Cargo : **Abogado y socio de Pazos Ikehara Abogados, profesor de Derecho en la Universidad Privada del Norte y la Universidad Científica del Sur.**
Fecha : **18/10/2023**

Premisa: La interceptación de datos informáticos es muy común hoy en día, la cual produce diferentes tipos de delitos, sus víctimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen.

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. **Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos?**
   Sí, pero, se tiene que entender que dichas "medidas" son transitorias: Con el desarrollo de la tecnología, se genera igualmente nuevas formas de criminalidad; por ello, la dificultad de establecer medidas que limitan o previenen la intercepción de datos.

2. **Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar:**
   Existen herramientas para prevenir como la utilización de programas de cifrado o de correos electrónicos alternativos; pero, se requiere tener presente,

igualmente, atender las recomendaciones de expertos en seguridad informática: Hoy en día, así como las empresas contratan agentes de seguridad personal para sus funcionarios, también contratan personal de seguridad informática para la prevención de sustracción de información.

3. **Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar.**
   Sí, se puede decir que dentro de todo son proporcionales al acto delictivo.

4. **¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar.**
   Existen varios factores: Por ejemplo, la falta o insuficiencia logística y de material humano para la detección, persecución y sanción del delito; pero, también, por la falta de conocimiento y educación que tienen los usuarios del sistema.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. **¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar.**
   No se tiene, desde mi punto de vista, una regulación de mecanismos de prevención; y, me parece bien, pues, si fuese así se tendría la necesidad de estar modificando la ley de manera continua a causa de los avances tecnológicos.

6. **Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar:**
   Me remito a la respuesta antes brindada.

7. **Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?** El mayor estudio y difusión sobre

los riesgos del uso de los sistemas sin tomar o considerar a la prevención de ilícitos: Mientras más enterada o educada se encuentren los usuarios, se tendrán mayores probabilidades de prevenir o evitar delitos.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

8. **En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar.**
   Me remito a la respuesta brindada a la pregunta #3.

9. **¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar.** Dependerá del impacto o daño social que dichos delitos generen a los usuarios. Solo así podrá ver la idoneidad, necesidad y proporcionalidad estricta de alguna "mejora".

10. **¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos? Argumentar.**
    Me remito a la respuesta brindada a la pregunta #3.

FIRMA	SELLO

ANEXO N° 11: Guía de entrevista a Azucena Yenny Tolentino Galindo

GUÍA DE ENTREVISTA

TÍTULO: Medidas de Seguridad y la Interceptación de Datos Informáticos en la legislación Peruana 2021 - 2022.

Entrevistado : Azucena Yenny Tolentino Galindo
Cargo : Juez del Octavo Juzgado de Investigación Preparatoria Permanente de la Corte Superior de Justicia del Callao
Fecha : 15/06/2022

Premisa: La interceptación de datos informáticos es muy común hoy en día, la cual produce diferentes tipos de delitos, sus víctimas pueden ser personas adultas como también menores de edad. La ley N° 30096 sanciona a todos los delitos que se cometen por la interceptación de datos informáticos. Se sabe que existe medidas de seguridad para evitar esta interceptación, pero no todos los conocen.

OBJETIVO GENERAL

Determinar de qué manera las medidas de seguridad limitan la interceptación de datos informáticos en la regulación peruana 2021 - 2022.

1. **Desde su punto de vista ¿Cree que las medidas de seguridad que existen limitan de alguna manera la interceptación de datos informáticos? Argumentar.**

   Las medidas de seguridad no limitan la interceptación de datos, este delito se da por falta de cuidado con quienes se expone nuestra información personal, además del mal uso de las medidas de seguridad que existe, no solo depende de estas medidas si no de uno mismo.

2. **Bajo su experiencia ¿Qué medidas de seguridad conoce para evitar la interceptación de datos informáticos? usa alguna de ellas, ¿cuáles? Argumentar:**

Las más común es usar una contraseña, guardar información en la nube, antivirus actualizado, las que uso son las antes mencionadas, siempre es recomendable cambiar de contraseña con datos que nadie pueda conocer y mantener actualizados todas las medidas de seguridad que se usan.

3. **Desde su punto de vista ¿Cree que las sanciones que se dan en la ley N° 30096 son las adecuadas? ¿Por qué? Argumentar.**

   No, las penas o sanciones que están establecidas en la ley N° 30096 no causan temor a los delincuentes, aunque son reprimidos siguen cometiendo este delito sin importarles las consecuencias, esto puede ocurrir porque las sanciones o penas que se les da son leves o en su momento no fueron detenidos por falta de pruebas.

4. **¿Por qué cree Ud. que se siguen cometiendo el delito de interceptación de datos informáticos? ¿Qué se podría hacer para evitarlo? Argumentar.**

   Este delito se sigue cometiendo no solo en el Perú sino ocurre en todos lados, en mi opinión es porque las sanciones que da nuestra legislación son leves y toma tiempo encontrar al delincuente, al ocurrir este delito por medio de la tecnología toma tiempo identificar al sujeto que realizo la interceptación de datos informáticos, por lo que la pena no se le puede dar inmediatamente.

OBJETIVO ESPECÍFICO 1

Determinar las medidas de seguridad adoptadas por la regulación peruana para evitar la interceptación de datos informáticos

5. **¿Cuáles son las medidas de seguridad que ha tomado la legislación peruana ante el delito de interceptación de datos informáticos? Argumentar**

   No hay ninguna medida de seguridad para evitar este delito, ya que depende de cada uno como protege su información con el avance de la tecnología, lo que si hay es una ley creada por la legislación peruana para castigar a los delincuentes que cometan el delito de interceptación de datos informáticos,

es la ley N° 30096 (Ley de Delitos Informáticos) con el único objetivo de prevenir y sancionar los delitos cometidos por medio de la interceptación de datos informáticos.

6. **Desde su perspectiva, ¿cree que las medidas tomadas son las correctas? ¿Por qué? Argumentar:**
   Las medidas de seguridad que uno tome dependen a sus conocimientos sobre la existencia de las medidas de seguridad que existen, ya que la sociedad de manera independiente ve como protege o que medidas aplica al momento de usar la computadora, celular, etc., o al momento de compartir su información.

7. **Desde su punto de vista, ¿Qué otras medidas se pudieron tomar ante la interceptación de datos informáticos?**
   Creo que las medidas que existen hoy en día son pocas conocidas, las cuales se deberían hacer conocer a toda la sociedad, ya sea por medio de charlas, cursos gratuitos, etc., claro que esta la ley N° 30096, pero esta solo castiga a los que cometen el delito.

OBJETIVO ESPECÍFICO 2

Determinar las sanciones que se dan por la regulación peruana para el delito de interceptación de datos informáticos.

8. **En base a su experiencia, ¿cree que las sanciones que se da por la legislación peruana son las correctas? ¿Por qué? Explicar**
   No, en mi opinión personal creo que deberían ser más severas, quizás así disminuya el delito de interceptación de datos informáticos.

9. **¿Cree que se puede mejorar estas sanciones? ¿Cómo? Argumentar**
   Claro que sí, es cuestión de que nuestros representantes dialoguen y lleguen a un acuerdo, también que pidan la opinión a la sociedad ya sea por encuestas o de otra forma, de esta manera también se podrá observar que tanto conocen del tema.

10. **¿Qué se debería hacer para que se disminuya el delito de interceptación de datos informáticos? Argumentar**

Tener cuidado con la información que cada uno comparte en sus redes sociales, asimismo cuidar a los menores de edad, porque son ellos los que están mas expuestos al momento de compartir su información.

FIRMA	SELLO