FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

“Delitos Cibernéticos y Confidencialidad en las Redes Sociales, Ica - 2020”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Pardo Echegaray, Jahir (ORCID: 0000-0002-5728-314X)

ASESOR:

Mg. Vilela Apon, Rolando Javier (ORCID: 0000-0002-5370-5608)

LÍNEA DE INVESTIGACIÓN:

Derecho penal, procesal penal, sistema de penas, causas y formas del fenómeno criminal.

LIMA - PERÚ

2021

Dedicatoria

Quiero dedicar además esta tesis a mis familiares, a mis hermanas por ser esas amigas incondicionales, por ser las luces que iluminan mi día a día y agradezco hoy en día. Por último quiero dedicar esta tesis a mis padres José y Alicia, gracias a su apoyo y aliento incondicional puedo culminar mis sueños".

Agradecimiento

Deseo agradecer a cada una de las personas que han estado presente en mi vida de los cuales me enseñaron y me dieron lecciones de vida que me hicieron una persona de cada vez mejor.

También a mi enamorada que me ha ayudado a cumplir mis anhelos durante este largo trayecto, y porque sé que estará ahí alentándome cada día y así concrete cada uno de mis sueños, porque nunca se deja de soñar.

Índice de contenidos

Carátula

Dedicatoria ii

Agradecimiento iii

Índice de contenidos iv

Índice de tablas v

Resumen vi

Abstract vii

I. INTRODUCCIÓN 1

II. MARCO TEÓRICO 4

III. METODOLOGÍA 12

3.1. Tipo y diseño de Investigación 12

3.2. Categorías, Subcategorías y matriz de categorización 13

3.3. Escenario de estudio 16

3.4. Participantes 16

3.5. Técnicas e instrumentos de recolección de datos 18

3.6. Procedimiento 20

3.7. Rigor científico 20

3.8. Método de análisis de datos 20

3.9. Aspectos éticos 21

IV. RESULTADOS Y DISCUSIÓN 22

V. CONCLUSIONES 43

VI. RECOMENDACIONES 44

REFERENCIAS 45

ANEXOS 56

Índice de tablas

Tabla 1 - Matriz de categorización 15
Tabla 2 - Lista de entrevistados - Abogados Litigantes, especialistas en Derecho Laboral 17
Tabla 3 - Validación de instrumentos – Guía de entrevista 19

RESUMEN

La presente investigación denominada “Delitos Cibernéticos y Confidencialidad en las Redes Sociales, Ica-2020”; tuvo como objetivo determinar como la información ya sea de administración pública, privada o personal dentro del ámbito informático pueden ser utilizados con el fin de la violación a la intimidad y utilizados de forma ilícita para la realización de actos delictivos.

La metodología empleada en el estudio fue de enfoque cualitativo, contando con un diseño de teoría fundamentada. Asimismo, se utilizó como instrumentos de recolección de datos a la guía de entrevista y guía de análisis documental.

La conclusión a la que se arribó fue que, se puede expresar que existe una sustancial necesidad legal en cuanto al aspecto de la titilación de los delitos informáticos, como tenemos la incautación de información, la intimidad personal en las redes sociales, tráfico ilegal de datos, las propuestas a los niños, niñas y adolescentes con fines sexuales por medios tecnológicos, fraude informático, suplantación de identidad y abuso del mecanismo informático y a ello deben considerarse con penas más vigorosas ya que en el presente son pocos los casos que prosiguen su curso legal y en mayor parte estos son archivados, lo cual resultaría muy perjudicial para ambas partes.

En ese sentido es necesario que las nuevas prácticas que los facinerosos informáticos emplean en nuestro país están a la mano de los pasos agigantados que la tecnología viene creciendo a diario, a pesar de ello existen bases legales a partir de las cuales se puede combatir las diferentes modalidades pero mas no en su totalidad de estas; es así que en base a lo mencionado se tiene que el fin es determinar los delitos informáticos cometidos y actualizados el día a día a través de la red del internet y redes sociales y saber qué tipo de tratamiento se puede brindar ante estos casos ya sea en el Poder Judicial y Ministerios que existen en el Perú .

Palabras clave: *delitos cibernéticos, tráfico ilegal de datos, confidencialidad, fraude informático, suplantación de identidad.*

ABSTRACT

The present investigation called "Cyber Crimes and Confidentiality in Social Networks, Ica-2020"; Its objective was to determine how information, whether from public, private or personal administration within the computer field, can be used for the purpose of violating privacy and used illegally to carry out criminal acts.

The methodology used in the study was of a qualitative approach, with a grounded theory design. Likewise, the interview guide and document analysis guide were used as data collection instruments.

The conclusion reached was that, it can be expressed that there is a substantial legal need regarding the aspect of the titling of computer crimes, such as the seizure of information, personal privacy in social networks, illegal data traffic , Proposals to boys, girls and adolescents for sexual purposes by technological means, computer fraud, identity theft and abuse of the computer mechanism must be considered with more vigorous penalties since at present there are few cases that continue their legal course and for the most part these are archived, which would be very damaging for both parties.

In this sense, it is necessary that the new practices that computer criminals employ in our country are hand in hand with the leaps and bounds that technology has been growing daily, despite this, there are legal bases from which it is possible to combat the different modalities but not in its totality of these; Thus, based on the aforementioned, the purpose is to determine the computer crimes committed and updated on a daily basis through the internet and social networks and to know what type of treatment can be provided in these cases either in the Judicial Power and Ministries that exist in Peru.

Keywords: cybercrime, illegal data traffic, confidentiality, computer fraud, identity theft.

I. INTRODUCCIÓN

En la actualidad, la llamada Sociedad Informática o Sociedad del Riesgo, en la que principalmente se predomina por el gran uso de las tecnologías de la Informática, tal fenómeno que es refrendado por el Derecho informático y su Ley de Delitos Informáticos - Ley N° 30096 y el Derecho Penal, en el caso del Derecho Informático suministrando conocimientos conforme al gran avance científico y en el caso del Derecho Penal estudiando los delitos informáticos en su asepsia política, sin siquiera afligirse por definir o precisar los tipos penales.

En nuestro Perú, con el pasar de los dias se han ido promulgando leyes, que han tenido como punto fijo de prevenir dichas conductas ilícitas, así como también el sancionarlas, y en ese sentido no ha pasado por demás los delitos cibernéticos y/o delitos informáticos, que se tiene como supuesto afectar el sistema y las bases de datos informáticas, que tienen como finalidad el afectar los bienes jurídicos, libertad sexual, entre otras, que afectan directamente a la sociedad.

En tal sentido la población en general se ve afectada por los ciberdelincuentes, cuando personajes ajenos, con la finalidad de obtener beneficios propios o para terceros agentes, de manera ilícita infringe los sistemas de seguridad de nuestros sistemas financieros, redes sociales, sistemas de autorización laborales, entre otros; con el fin de la obtención de información secreta, clonación de tarjetas, robo de datos personales, imágenes, videos, entre otras, y ocasionar daños a la población.

Si bien es cierto en la actualidad ha revolucionado la modernidad de diferentes sistemas públicos, así como también sistemas privados, siendo uno de estos los que generan las operaciones de accesos a diversos sistemas en segundos o minutos, postura que la población de hace 20 años no imaginaria realizar operaciones y tener accesos a sus cuentas de diferentes índoles de cualquier parte del mundo, dejándose así las limitaciones y así apegándose al mundo cibernético.

Conforme a lo señalado, los robos de datos personales, contraseñas, y diferentes datos para accesos personales se han dejado de lado, pues ya no es necesario que los delincuentes tengan armas blancas para que comentan sus delitos ya que hoy en día ya utilizan sus mecanismos cibernéticos para cometer sus fechorías y así ocultando su identidad del que ejerce estos sus fechorías y así no atenta contra la vida, libertad y salud de las personas.

Es así que una de las principales razones para que la ciberdelincuencia aumente cada día, es la dificultad que se tiene para la identificación y ubicación de los autores, y así quedando muchos de estos delitos cometidos en la impunidad, generando una enorme inconformidad de parte de la sociedad y así la pérdida de confianza en la justicia eficiente y oportunidad del Perú, en ese sentido de acuerdo a lo señalado, es necesario que nuestro sistema de justicia, proteja a los demandantes.

Con estos antecedentes, el problema del presente trabajo de investigación, se relaciona con los delitos informáticos, ya que lesionan los derechos de los ciudadanos, y muchos de estos casos, los delitos quedan en la impunidad, por la enorme dificultad que se tiene para descubrir a los autores.

Por lo tanto, el alcance del ciberdelito es mayor, pudiendo incluir delitos tradicionales como fraude, robo, extorsión, pornografía y falsificación; qué computadoras y redes informáticas se utilizan como medio para llevar a cabo estos actos.

En general el presente trabajo de investigación se trata de desarrollar temas como son, los delitos informáticos, características, temas relacionados a la intimidad, como se ve afectada la sociedad y los efectos positivos y negativo de las leyes peruanas ante estos hechos.

II. MARCO TEÓRICO

Para el mayor sustento del presente trabajo, examinaremos los diferentes tipos de fuentes en el entorno nacional, como son las siguientes:

Por su parte, Villavicencio (2014) considera que:
Se entiende por ciberdelincuencia una conducta encaminada a evadir los sistemas de equipos de seguridad, es decir, inmiscuirse en un sistema informático, de correo electrónico o de datos a través de un código de acceso; comportamiento típico que solo se puede lograr a través de la tecnología.

Al respecto, Ramírez y Castro (2018) argumentaron que el delito cibernético o informático "es cualquier acto ilegal que se produce a través de medios informáticos o intentos de manipular o destruir computadoras, redes de Internet o medios electrónicos".

Según Besares (2015) señala que el delito informático
Es un acto ilegal y criminal típico que afecta la seguridad informática y la privacidad humana a través del procesamiento fraudulento de datos, que es diferente de otros casos de delitos informáticos o electrónicos.

Asimismo, Téllez (2012) Son "actitudes ilegales que usan la cibernética como herramienta o propósito, o actos típicos, ilegales y criminales que usan la cibernética como instrumento o propósito".

Finalmente, Blossiers (2018), determina que "estos actos ilegales de uso indebido de cualquier medio informático están dentro del alcance de las sanciones de la ley penal"

Es así que, en cuanto a los antecedentes internacionales, se logra comprobar que existen las investigaciones que se presenta a continuación y que tienen relación en la línea de la presente investigación.

Los delitos cibernéticos en la modalidad de hurto, fraude, estafa y sabotaje.

Hurto cibernético: La apropiación indebida o robo de software y datos: en este caso, el sujeto accede a una computadora ajena o la sesión de otro usuario ejecutando un comando de copiar o cortar, borra archivos de computadora y luego guarda el contenido con su propio soporte. (Alcívar, Domenech y Ortiz, 2015, p. 45).

Fraude cibernético: Vásquez, Regalado y Guadron (2017), señalaron que el fraude informático se refiere a causar pérdidas patrimoniales a terceros mediante la manipulación de datos informáticos o interfiriendo con el funcionamiento de los sistemas informáticos, y su finalidad es obtener de forma ilegal beneficios económicos para uno mismo o un tercero.

Sabotaje cibernético: Bashir y Khalique (2016) argumentan que la destrucción se considera uso no autorizado de instalaciones informáticas, alteración o destrucción de información, destrucción de archivos de datos y destrucción deliberada de sistemas informáticos. La computadora debe estar protegida contra manipulaciones para evitar cualquier inconveniente.

La clasificación de delito informático es diversa, en muchos casos se refiere al mismo tipo de delito, pero con diferentes nombres, al respecto, Loredo y Ramírez (2013) citando a INTERPOL señalan como delitos informáticos los siguientes:

- Ataques contra sistemas y datos informáticos.
- Botnets (redes de equipos infectados controlados por usuarios remotos).
- Difusión de virus.
- Distribución de imágenes de agresiones sexuales contra menores.
- Estafas a través de Internet.
- Intrusión en servicios financieros en línea.
- Phishing (adquisición fraudulenta de información personal confidencial).
- Usurpación de la identidad.

Las Naciones Unidas (2013), señalan lo siguiente en relación a la concientización:

- La mayoría de los usuarios individuales de Internet han tomado precauciones de seguridad básicas.

- Todas las partes interesadas enfatizan la importancia continua de las campañas de concienciación pública, incluidas las campañas que cubren las amenazas emergentes y las campañas dirigidas a públicos específicos (como los niños).
- La educación del usuario es más eficaz cuando se combina con un sistema que ayuda a los usuarios a alcanzar sus objetivos de forma segura.

Pardo (2018) en su investigación señala las principales características de los delitos cibernéticos, haciendo recuento que podemos identificar lo siguiente en delitos informáticos:
- Es de carácter internacional, porque la proximidad no es condición necesaria para la comisión de estos delitos.
- El alcance judicial de estos delitos se ha visto reducido por la escasez y reducción de denuncias, alcance regulatorio, fiscales especializados y normativas en derecho penal internacional.
- Por lo general, son malintencionados o deliberados, pero también pueden ser culpables.
- Pueden provocar mucha corrupción económica grave, porque suelen verse afectadas grandes cantidades de dinero o activos.
- Debido a sus especiales características técnicas, presenta serios problemas en la demostración.
- Requiere poco espacio y tiempo, pues estos delitos se pueden llevar a cabo en pocos segundos o con un clic. Además, generalmente no se requieren grandes equipos o máquinas informáticas porque se puede realizar a través de un teléfono móvil de bolsillo.
- Estos son comportamientos oportunistas, porque los delincuentes informáticos se benefician del avance tecnológico acelerado, las víctimas están en todas partes y carecen de conocimientos profesionales.
- Estos son comportamientos profesionales, y los ciberdelincuentes se aprovechan de sus comportamientos delictivos dentro del ámbito de las víctimas que utilizan los medios informáticos para trabajar.
- Este es un delito de reciente aparición, cuyo número aumenta constantemente, y se está volviendo más especializado y complicado.
- Estos son delitos de cuello blanco, porque el sujeto de la actividad debe ser una persona con conocimientos de informática y tecnologías de la información.

Las Naciones Unidas (2013), señalan lo siguiente en relación a la prevención y estrategias:

-Existencia de legislación o políticas nacionales para prevenir el ciberdelito. Otro 20% de los países están haciendo planes.

-Las buenas prácticas incluyen la promulgación de leyes, el liderazgo eficaz, el desarrollo de la justicia penal y las capacidades de aplicación de la ley, la educación y la conciencia, el desarrollo de una sólida base de conocimientos y la cooperación entre el gobierno, el sector privado, la comunidad y la comunidad internacional.

-Una estrategia nacional que incluye componentes como la sensibilización, la cooperación internacional y las capacidades de aplicación de la ley.

-Establecer una alianza público-privada para prevenir y combatir los ciberdelitos.

En cuanto a los derechos constitucionales, Correa (2016) considera que:

La constitución es una ciencia social. Como hemos visto, su campo de acción se encuentra entre el poder de la existencia y la responsabilidad de la existencia. Su propósito fundamental es el estudio de la constitución política. Su propósito es confirmar, unificar y sistematizar el ordenamiento jurídico del país.

Herrera (1987), afirma que el Derecho es "un código de conducta obligatorio, formulado por personas que viven en sociedad, está destinado a regir las relaciones sociales, el orden y la justicia". En cuanto al derecho constitucional,

La Defensoría de la Niñez (2017), señala que:

El concepto de vulneración de derechos corresponde a toda vulneración de los derechos de las personas establecidas, que puede constituir o no delito, según nuestra legislación. En cualquier caso, cualquier violación de derechos es grave, por lo que los países deben tomar todas las acciones para evitar que ocurran estos incidentes y brindar mecanismos para restituir los derechos después de la violación de derechos.

García (1999), sostiene que:

[…] el Derecho Constitucional estudia las instituciones y categorías legales y políticas relacionadas con el ejercicio, autoridad, relación y control de los poderes

públicos asignados a territorios y poblaciones específicas; así como los derechos, obligaciones y garantías de las personas relacionadas con las instituciones políticas. (p.203).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación:

Tipo de investigación. – Este trabajo de investigación utiliza un método cualitativo, pues el propósito de estudiar un tema social desde la perspectiva de los participantes es obtener y recolectar información para formar una base de datos; la investigación proviene del aprendizaje, es decir, el propósito principal es para el beneficio de conocimientos sobre el punto de los Delitos informáticos y las vulnerabilidades que se tiene en las redes sociales.

Diseño de investigación. - El enfoque planteado en el presente informe de investigación es cualitativo encuadrado en el diseño en la teoría fundamentada, debido que el estudio se realiza dentro de un Poder Judicial, donde para la obtención de la información se interactúa con las personas que laboran dentro de dicha institución; asimismo, es preciso señalar que con lo expuesto se busca el desarrollo de la información recabada.

Por lo tanto, según el contenido mostrado, debemos tener claro que se aplica la teoría fundamentada, porque en base a toda la información y preguntas seleccionadas, se aplica a la teoría relacionada con el propósito de la investigación.

3.2. Categorías, Subcategorías y matriz de categorización apriorística.

TABLA 1. *Matriz de categorización apriorística*

Categoría	Definición Conceptual	Definición Operacional	Subcategorías
Delitos Cibernéticos	Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. (Articulo 1 de la Ley Nª30096)	Dependiendo de su tipificación o no tenemos que, los delitos cibernéticos son "actitudes ilìciad en que se tiene la cibernética como instrumento o fin" o las "conductas típicas, antijurídicas y culpables en que se tiene a la cibernética como instrumento o fin". Tellez (2018)	Phishing
			Interceptación de datos personales.
Ciberdelincuencia en Redes Sociales	Son actos ilícitos realizados por un uso indebido de la tecnología, amenazando la privacidad de información de terceros, destruyendo o extrayendo cualquier tipo de datos almacenados en el servidor. Representa un comportamiento completamente ilegal que pretende destruir a los usuarios de medios electrónicos y redes de Internet, y en algunos casos, difamar y chantajear a los usuarios. Acosta (2020).	Presentan las características ideales para aumentar el riesgo de conductas relacionadas con el delito, y los delitos de odio son un área afectada por la expansión del derecho penal. Sin embargo, los tribunales españoles no respondieron de manera consistente y predecible, lo que demuestra la seria aplicación de tipos de delitos alternativos terroristas que atentan contra el derecho a la libertad de expresión y el principio de castigo proporcional. Tamarit Sumalla (2018)	Extorción
			Filtración de conversaciones.

3.3. Escenario de estudio

El antecedente de la investigación fue en la ciudad de Ica, donde surgió el problema, y se estableció por el espacio físico donde se realizó la entrevista. Es necesario señalar que la entrevista involucra a profesionales calificados en el campo y donde se realizó la entrevista. Cabe mencionar que el escenario de la anterior entrevista es el domicilio del personal del Poder Judicial, pues los peritos decidieron desarrollarlos allí porque es imposible estar en el despacho del Poder Judicial debido a la pandemia de Covid.

3.4. Participantes

Es importante determinar que los profesionales que participarán en este proyecto de investigación son jueces del Poder Judicial, quienes cuentan con amplia experiencia en el campo penal y tienen mucho conocimiento sobre el comportamiento de la Ley N ° 30096 de la Ley de Delitos Informáticos. Podrán explicar cuestiones relacionadas con el plazo establecido.

Conforme a lo expresado, por lo que queda establecido que los participantes son los siguientes:

TABLA 2. *Participantes*

Nombres y Apellidos	Institución	Escenario de estudio	Años de experiencia
SANDRA FERNANDEZ VALENCIA	PODER JUDICIAL	CERCADO DE ICA	10
DIANA VENTURA CALDERON	PODER JUDICIAL	CERCADO DE ICA	06
LUZMILA VIOLETA ECHEGARAY BERNAOLA	PODER JUDICIAL	CERCADO DE ICA	09
GINA MARIÑO CALDERON	PODER JUDICIAL	CERCADO DE ICA	02
TITO OYANGUREN RAMOS	PODER JUDICIAL	CERCADO DE ICA	10
FRANCISCO BENAVENTE QUISPE	PODER JUDICIAL	CERCADO DE ICA	10
LIZBETH PIMENTEL DIAZ	PODER JUDICIAL	CERCADO DE ICA	10

Fuente: elaboración propia.

3.5. Técnicas e instrumentos de recolección de datos

En la investigación cualitativa, al recolectar datos, casi siempre se generan otras ideas para recolectar otras ideas (Bansal et al., P. 1193). Sin embargo, se utilizaron estas técnicas y herramientas. En cuanto a las técnicas, se dispone de entrevistas porque según el juicio de Hernández (2014), se examinan las vivencias de las personas asociándolas a tareas habituales o laborales, con especial énfasis en las actividades e interrelaciones que permean el medio natural, dejando de lado los escenarios artificiales La modificación resultante (p. 188). Según Marvasti (2019), el método más común de recopilación de datos en métodos cualitativos son las entrevistas (p.6).

El instrumento utilizado es la guía de entrevistas. Una de las técnicas aplicadas es el análisis de la literatura, a través del cual se utiliza la guía de análisis de la literatura como instrumento para recolectar información de las fuentes de la literatura.

Tabla 3. Validación de instrumentos – Guía de entrevista

	Validación de Instrumentos		
Instrumento	**Datos generales**	**Cargo o Institución**	**Porcentaje**
Guía de Entrevista	Gamarra Ramon, Jose Carlos	Docente UCV-Lima Norte	95%
	Luca, Aceto	Docente UCV-Lima Norte	95%
	Mogollon Longa Johnny William	Docente UCV-Lima Norte	95%
	Promedio		95%

3.6. Procedimiento

Para poder obtener la información señalada en el presente trabajo de investigación, me eh apersonado a los domicilios de los abogados que trabajan en el Poder Judicial ya que por motivos de seguridad ante la pandemia no se pudo ingresar al Poder Judicial, en ese sentido se ha procedido a entrevistarse los diferentes funcionarios del Poder Judicial; en ese sentido, se ha optado por utilizar las bibliotecas virtuales como presenciales para obtener artículos indexados relacionados al caso en concreto.

3.7. Rigor científico

La investigación del cambio cualitativo se realiza de manera justa e involucra diferentes teorías cognitivas y herramientas para asegurar la efectividad de esta investigación; el rigor es un aspecto importante, porque es la piedra angular de la investigación, se refiere a la existencia del orden de investigación, el alcance

del sistema, y la estructura de la investigación y conducen al resultado final de la investigación.

3.8. Método de análisis de datos

Este es un programa que recopila, organiza y clasifica la información relacionada con un tema específico obtenida por los investigadores y saca conclusiones de ella; el análisis de datos tiene una etapa orientada a obtener resultados más precisos.

En este sentido, de lo anterior se desprende que la información obtenida primero debe ser revisada y sintetizada, lo que significa utilizar la más importante para que nos ayude a obtener los resultados de la investigación

Por otro lado, toda la información publicada debe ser utilizada para investigaciones, porque permite sacar resultados en base a todo el proceso de investigaciones y en definitiva sacar conclusiones correctas.

3.9. Aspectos éticos

Este trabajo de investigación es elaborado con base en los parámetros, información válida y fuentes confiables que brinda la Universidad del Cesar Vallejo, y el consultor ha realizado un análisis detallado del mismo; nuevamente, el desempeño de este trabajo es ético porque no viola, no violar ninguna ley, reglamento o buenas costumbres.

IV. RESULTADOS Y DISCUSIÓN

En el presente trabajo de investigación se indicará la parte del trabajo de investigación o informe científico, que como se puede apreciar describe el significado de los hallazgos obtenidos, comparados y resaltados con las investigaciones realizadas. Si bien es cierto se propone una validación, verificación o rechazo, también se debate con los resultados que se obtuvieron. Es así que, que es la parte de gran importancia respecto a la investigación, ya que es el fundamento principal del estudio.

Siendo así, en el presente caso se detallaron los presentes resultados que se obtuvieron de la guía de entrevista dirigida a algunos funcionarios del Poder Judicial de la ciudad de Ica, siendo la descripción del los siguientes puntos:

Objetivo General: Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales; en relación a este objetivo se planteó las siguientes preguntas:

1. ¿Cree usted que los delitos cibernéticos afecten más en los menores de edad?

Pimentel (2021), detallo que los menores de edad son los que tienen más exposición a las redes sociales sin control ni supervisión de un adulto.

Por parte de Fernandez (2021), manifestó que los menores de edad no están conscientes de los peligros que impliquen exponerse en la web.

Asimismo Mariño (2021), señalo que los menores de edad son usuarios constantes de las redes sociales y son vulnerables a delitos por medios cibernéticos.

De la misma manera, Echegaray (2021), manifestó que a través de ellos muchas personas engañan a los menores que son vulnerables por su edad.

Ventura (2021), señalo que si les afecta ya que no tienen demasiadas experiencia usando redes por lo que sufrir de delitos cibernéticos es mucho mas fácil y común.

Siguientemente Oyanguren (2021), manifiesta que ellos no tienen la experiencia de una persona adulta.

Y finalmente Benavente (2021), señalo que si porque son más fáciles de captar.

2. ¿Cree usted que la ley de delitos informáticos necesita alguna modificatoria con el gran avance que tiene la tecnología y los ciberdelincuentes?

Fernandez (2021), señala que si necesitan de modificatorias de acuerdo a la tecnología que no avanza.

Por otro lado Mariño (2021), manifestó que la ley vigente necesita una modificatoria inmediata, ya que no se adecua a la realidad, siendo eficaz.

Asimismo, Ventura (2021), señalo que las leyes cambian con el pasar del tiempo y con la tecnología que va a paso acelerado y con ello los diversos métodos.

Echegaray (2021), en su manifestación señala que si, porque debería haber hecho una ley que prohíba ciertas páginas que pueden ingresar los menores y poner más drástica para las personas que los engañan.
Es asi que Oyanguren (2021), señalo que tienen que actualizarse de acuerdo a como se va desarrollando cada ámbito de nuestra vida diaria.

3. De acuerdo con usted, ¿De qué forma afectan los delitos cibernéticos?
Mariño (2021), manifiesta que afecta gravemente a la integridad de un sector vital de la sociedad.
Por otra parte Ventura (2021) señalo que vulneran la privacidad de las personas y exponen a sufrir dichos delitos, infringen los términos de privacidad y seguridad de algunas paginas webs.
Asimismo Fernandez (2021) detallo que afecta directamente a la intimidad de documentos, conversaciones, secretos de las personas naturales y jurídicas.
Echegaray (2021), señala que si afectan, porque muchas veces a través de ellos a muchos menores, a través de su vulnerabilidad, además a las personas que desconocen de este sistema y se les engaña y es más clonar tarjetas.
Por parte de Pimentel (2021) señalo que afectan considerablemente a la población niños, adolescentes con el tema de estafas, prostitución, pornografía, entre otros.
Oyanguren (2021) detallo que las personas que le hicieron el delito cibernético es dañada de forma psicológica y también de repente económica.
Finalmente Benavente (2021) manifestó que de forma psicológica y hasta económica.

Objetivo Especifico 1: Analizar de qué manera el Phishing influye en la interceptación de datos personales, por lo que se realizaron las siguientes preguntas:

4. ¿Considera Ud. que el uso del el Phishing influye en la interceptación de datos personales?
Mariño (2021), señala que desde su punto de vista hasta cierto punto ya que es una herramienta limitada.
Echegaray (2021), manifiesta que no conoce sobre el phishing.

Por otro lado Fernandez (2021) declaro que si influye ya que el phishing es el delito de engañar a las personas para que compartan información confidencial.
Ventura (2021), expuso que si porque vemos como esta modalidad roba los datos personales al hacerse pasar por alguien.
De la misma forma Pimentel (2021), expuso que si porque es un mecanismo muy difícil de detectar.
Finalmente Oyanguren (2021) confirmo que si, ya que contribuyen a la captación de datos.

5. Según su experiencia profesional, ¿Cuál considera que son los factores que se determinan sobre el uso del Phishing en la interceptación de datos personales?

Mariño (2021), señalo que la poca seguridad virtual, debido al pésimo labor del estado en control de las redes.
Fernandez (2021), manifestó que la confianza que le pueden dar hacia la otra persona y de esta manera engañar y lograr que le puedan dar su información personal.
Por otro lado Ventura (2021), declara que uno de los factores importantes es la inseguridad y confianza que tiene la victima al sufrir dicho delito.
Por tu parte Oyanguren (2021), señala que dar confianza a las personas que aún no se conocen puede contribuir a ello.
Benavente (2021), por su parte señala que afecta al ingresar datos en paginas falsas.
Finalmente Pimentel (2021), manifestó que el principal factor es la falta de información .

6. ¿Cree usted que en los últimos años se ha incrementado los casos de phishing

Mariño (2021), señalo que si, ya que este conocimiento se está esparciendo.
Fernandez (2021), manifestó que si se ha incrementado por el acceso a la tecnología.
Por su parte Ventura (2021), expuso que si en los últimos años se ha incrementado al ver que los ciudadanos tienen un mayor acceso a la tecnología.

Asimismo, Oyanguren (2021), exhorto que se ha incrementado porque la juventud de hoy aprende más rápido sobre las redes donde ellos son puntos débiles para estos casos.
Finalmente, Benavente (2021), señala que si, se ha incrementado ya que existen innumerables juegos que solicita el ingreso de datos personales.

Objetivo específico 2: De qué manera la extorción incide en la filtración de conversaciones. En relación a ello, se plantearon las siguientes preguntas:

7. ¿Cree usted que las extorciones del hoy en día son producto a la filtración de conversaciones?

Mariño (2021), señalo que si ya que son materiales privados con información que se pueden convertir en extorción.
Echegaray (2021), manifestó que no siempre porque muchas veces también las extorciones es por venganza.
Por otro lado Ventura (2021), declaro que si, para que algunas extorciones debe ser una información importante de dichas victimas para cometer el delito.
Del mismo modo Fernandez (2021),señala que si son producto a la filtración porque los extorsionadores deben tener una información importante sobre su privacidad del usuario.
Por otro lado Oyanguren (2021), manifestó que Si porque necesitan de ello para poder lograr su delito.
Finalmente Pimentel (2021), señala que si hoy en día han llegado una gran cantidad de denuncias referente al tema de extorción por filtración de conversaciones.

8. ¿Usted considera que la extorción cibernética debería tener una condena drástica?

Mariño (2021), señalo que debe tener una pena mayor a la extorsión normal.
Echegaray (2021), manifestó que para ver si a través de ello la gente tiene más cuidado y no cometiera delito.
Por otra parte, Fernandez (2021), declaro que debería ser de acuerdo al hecho.
También, Ventura (2021), contemplo que para ello va a depender de la gravedad del hecho.

Adicionalmente Oyanguren (2021), manifestó que si, ya que es un delito que perjudica al extorsionado.
Finalmente, Pimentel (2021), señala que si por eso es que lo siguen haciendo porque no hay condenas drásticas.

9. ¿Según su experiencia profesional, ¿Cuál considera que es el modus operandi de los ciberdelincuentes en la Región de Ica?

Mariño (2021), manifestó que es el Phishing.
Echegaray (2021), señala que a su criterio es la clonación de tarjetas.
Por otra parte, Ventura (2021), recalco que la modalidad es que buscan a víctimas de las zonas de bajos recursos donde desconocen estas modalidades de estafa y así cometer el robo de información.
Asimismo, Fernandez (2021), considera que la extorsión y el fraude.
De la misma forma Oyanguren (2021), señala que captar a menores de edad para realizarles trata de personas, fraude y sacar información.
Finalmente, Pimentel (2021), manifestó que identidades falsas en las redes sociales, así como también los números telefónicos.

Inventario de resultados de la guía de análisis de fuente documental.

Es así que es una forma fundamental la recopilación la información obtenida luego de poder analizar los documentos que se tiene como fuente para la investigación.

Objetivo General: Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales; en relación a este objetivo se analizaron los siguientes documentos:

Ley N° 30096 Ley de Delitos Informáticos

La citada Ley en el artículo 7 de la presente ley y Modificación de los artículos 162, 183-A y 323 del Código Penal, nos señala sobre la confidencialidad

Artículo 7.- Interceptación de datos informáticos Cualquiera que intercepte datos informáticos en transmisión no pública a través de tecnología de la información o la comunicación, los dirija a un sistema informático, se origine o ejecute en el sistema informático, incluida la radiación electromagnética, los datos

informáticos del sistema informático que transmite la información anterior, Ser reprimido de tres formas: Prisión fija por no menos de seis años. Cuando el delito cometido se encuadre en la confidencialidad, retención o confidencialidad de la información estipulada en el reglamento del caso, la privación de libertad no será menor de cinco a ocho años. Los delitos que pongan en peligro la defensa, la seguridad y la soberanía nacionales serán sancionados con pena privativa de libertad no menor de ocho años ni mayor de diez años.

Modificación de los artículos 162, 183-A y 323 del Código Penal Modificase los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos: "Artículo 162.- Interferencia telefónica Cualquiera que interfiera indebidamente o escuche una conversación telefónica será sancionado con pena de prisión de no menos de tres años y no más de seis años. Cuando el agente sea un funcionario público, será condenado a pena privativa de libertad no menor de cuatro años pero no mayor de ocho años de conformidad con lo dispuesto en los párrafos 1, 2 y 4 del artículo 36, y quedará inhabilitado. La pena privativa de libertad no menor de cinco años y no mayor de ocho años cuando el delito involucre información clasificada como secreta, reservada o confidencial según las reglas de la materia. Cuando un delito ponga en peligro la defensa y la seguridad nacional o la soberanía nacionales, la privación de libertad no será menor de ocho años y la mayor no excederá de diez años.

Objetivo Específico 1: Analizar de qué manera el Phishing influye en la interceptación de datos personales, por lo que se analizaron los siguientes documentos:

"(…) Artículo 7.- Interceptación de datos informáticos Cualquiera que intercepte datos informáticos en transmisión no pública a través de la tecnología de la información o la comunicación, los dirija a un sistema informático, se origine o ejecute en el sistema informático, incluida la radiación electromagnética, los datos informáticos del sistema informático que transmite la información anterior, Ser reprimido de tres formas: Prisión fija por no menos de seis años. Cuando el delito cometido se encuadre en la confidencialidad, retención o confidencialidad de la información prevista en el reglamento del caso, la privación de libertad no será menor de cinco a ocho años. Quienes pongan en peligro la defensa, la

seguridad o la soberanía nacional serán sancionados con pena privativa de libertad no menor de ocho años ni mayor de diez años (…)".

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente: "CUARTA. Para asegurar el intercambio de información, equipos conjuntos de investigación, transferencia de expedientes, interceptación de comunicaciones y demás actividades correspondientes para la implementación de esta ley, la Policía Nacional del Perú, Ministerio Público, Poder Judicial, Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores criminales del sector privado debe formular un acuerdo de cooperación operativa reformado dentro de los 30 días a partir de la fecha de vigencia de este documento o ley "

Objetivo Específico 2: De qué manera la extorción incide en la filtración de conversaciones, en ese sentido se establecieron lo siguientes documentos y en ese sentido observando la siguiente disposición:

"(…)DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

"Artículo 1. Marco y finalidad Esta ley tiene por objeto otorgar a los jueces la potestad constitucional para comprender y controlar las comunicaciones de las personas que sean objeto de investigaciones preliminares o judiciales a través del desarrollo legislativo. Las facultades estipuladas en esta ley solo podrán ser ejercidas para los siguientes delitos:

1. Secuestro.

2. Trata de personas.

3. Pornografía infantil.

4. Robo agravado.

5. Extorsión.

6. Tráfico ilícito de drogas.

7. Tráfico ilícito de migrantes.

8. Delitos contra la humanidad.

9. Atentados contra la seguridad nacional y traición a la patria.

10. Peculado.

11. Corrupción de funcionarios.

12. Terrorismo.

13. Delitos tributarios y aduaneros.

14. Lavado de activos.

15. Delitos informáticos.” (…)”

Se puede inferir que el ciberdelito puede causar un gran daño a la gente común en cualquier momento de sus vidas, porque no solo pueden convertirse en víctimas, por lo que deben estar preparados para proteger cuentas, ingresos, contraseñas, y no se debe confiar en las computadoras en Internet. , aunque la mayoría de las personas no se han convertido en víctimas de ningún delito informático, nadie puede asegurarnos que quienes aún no se han convertido en víctimas puedan convertirse en víctimas. El internet de hoy es tan importante, pero a pesar de ello, para obtener los resultados de la investigación se puede inferir que cualquier forma de uso de un sistema informático afectará la privacidad. En este sentido, es necesario proteger todos nuestros datos de terceras personas, ya que se puede evitar daños graves deliberadamente, para que no aprovechen la oportunidad, y comiencen a no ser perjudicados por diversos delitos e infracciones en Internet.

La tecnología aun se encuentra avanzando, así como también con mayores pasos agigantados la inseguridad social, es así que no hay que confiar en compras o brindar datos personales por internet o cualquier medio informático, ya que pueden llegar a ser paginas falsas por ende la mayor parte de la población que a sido victima nisiquiera se a dado cuenta de ello y es asi que en el presente existen una enorme cantidad de denuncias respecto a estos tipos de vulneraciones por las que pasa la población que aun no sabe de estos tipos de delitos.

El ingreso a realizar compras, brindar datos y redes sociales; cabe mencionar que es muy difícil investigar delitos informáticos, porque son demasiado difíciles de encontrar, y luego realizar una búsqueda detallada para verificarlo, pero hay expertos en informática que pueden a fondo investigación pero de esta forma se tiene que los peritos aun no se encuentran tan preparados a comparación de los ciberdelincuentes y sus pasos agigantados; el mundo en el que vivimos tiene avances y cambios tecnológicos asombrosos, por lo que para combatir el ciberdelito es muy necesario implementar fuertes sanciones. Para que el sujeto que comete tales delitos no cause ningún daño grave a la gente.

Dicho todo esto la seguridad de la población es lo principal para el estado que se pueda proteger de los ataques a la población, porque la seguridad y el bienestar de los ciudadanos está en riesgo todos los días, en este sentido está consagrado en nuestra Constitución. La mayoría de las personas se quejan de la seguridad de estos puntos de ciberdelincuencia proporcionados por el estado ya que prácticamente se encuentran abandonados en sus derechos con respecto a la tecnología.

Se puede enfatizar que la difusión de datos sí afecta directamente la integridad de las víctimas, porque su vida privada ha sido expuesta a la multitud, por lo que son conocidos por ellos. En este sentido, su privacidad y prestigio está en boca de toda la gente que trabaja en su privacidad.

Es de suma preocupación que un ciber infractor luego que haya cometido un delito cibernético llega a dar paso a los chantajes y extorsión de sus víctimas con la finalidad de perjudicar y llegar a obtener beneficio de la misma.

V. CONCLUSIONES

Nuestro Perú es un país en el cual se encuentra en constantes cambios que permiten las investigaciones y condenas por delitos cibernéticos, pero es necesario desarrollar, mejorar e implementar mecanismos para mantener dichas investigaciones en la dirección adecuada y capacitar continuamente a los profesionales dentro del marco legal adecuado.

La tecnología se encuentra avanzando rápidamente a nivel mundial pero a la misma vez ocasiona un sin número de formas para que los ciberdelincuentes puedan delinquir, con la utilización de los medios tecnológicos que estos manejan y es así que por ser de libre acceso la población termina confiando y añadiendo y brindando información personal donde no deberían hacerlo.

De acuerdo con los datos obtenidos, de la investigación se desprende que los datos que atentan contra la persona afectan directamente la integridad, y la conducta delictiva de la persona que comete delitos informáticos es muy diferente a la persona que comete cualquier otro delito. En el momento, los perpetradores son personas con formación académica relevante que pueden utilizar fácilmente el sistema informático e intentar eliminar todas las pruebas de la misma forma, por lo que son difíciles de encontrar.

Por lo tanto, para aquellos que no tienen estos conocimientos básicos de informática, es más probable que se conviertan en víctimas de delitos informáticos, esta parte de la población puede llegar a ser la parte más afectada y si en algún momento dado llegan a manejar un sistema informático y no se le ha dicho de manera adecuada que utilice la tecnología responsable del mismo conforme a la encuesta se deduce que se debe implementar mayor seguridad en las redes para que así los ciberdelincuentes no lo utilizarán y causarán graves daños económicos y psicológicos, porque hay que recordar que cualquiera puede convertirse en la próxima víctima de un caso.

Por ello, el delito informático forma parte del derecho penal peruano, el cual tiene como objetivo proteger a nuestra población de acuerdo con la Constitución y traducirlo en sanciones y normas legales que deben ser respetadas y garantizadas, por lo que el demandado debe implementar medidas más estrictas contra quienes cometan tales delitos.

En este sentido, según los informes relacionados con casos de seguridad y los informes de vulnerabilidad, el ciberdelito está creciendo muy rápido y los enormes costos involucrados ya se encuentran en una valiosa desventaja para la empresa y el público en general.

VI. RECOMENDACIONES

Llegar a la incentivación a la población y así como también a los profesionales de todo ámbito para capacitarlos en el tema de delitos informáticos y vulnerabilidades en las redes sociales, a fin de promover las investigaciones correspondientes a nivel legal, el Estado debe proponer un seminario o plan de capacitación al público en general.

Si en caso son víctimas de un delito cibernético, deben informar a la policía o a la fiscalía del incidente para que puedan realizar las investigaciones pertinentes para proteger los derechos de los afectados.

Por lo tanto, para mantener la información protegida, es necesario el consejo de una persona con amplios conocimientos informáticos, de modo que pueda ayudarlo a garantizar que toda la información que ingrese esté respaldada y se mantenga confidencial.

Se deben implementar programas y anuncios para advertir de delitos informáticos, porque estos delitos requieren de minuciosas investigaciones para descubrirlos, si las personas no tienen suficientes advertencias o preparativos, será más difícil dar soluciones o reducir el número de casos. Al crimen informático.

Se debe buscar conciencia en nuestra sociedad, advertencias sobre el uso de tecnologías existentes en los programas de televisión, por lo que se considerarán las medidas necesarias para evitar que los ciberdelincuentes se infiltran en los sistemas informáticos protegidos.

Existe un debate abierto en nuestras doctrinas legales y agencias reguladoras sobre los delitos informáticos y sus consecuencias para la sociedad, porque es indiscutible que este tema es muy importante, por lo que perjudicará a toda la comunidad. Población, por lo que hacer referencia a los pasos señalados en la ley sería una alternativa eficaz.

El pueblo peruano debe utilizar diversas herramientas técnicas para facilitar estos casos, en lugar de herir a otros, porque al herir a otros, serán irresponsables y cometerán delitos, aunque llegue y afecte a las personas a las que se dirigirá, se callará.

REFERENCIAS

VIII Bibliografía consultada para elaborar el proyecto

Alcívar, C., Domenech, A., y Ortiz,M. (2015). *La seguridad jurídica frente a los delitos informáticos. Revista de Investigación Jurídica*. 10(12), 41 http://revistas.upagu.edu.pe/index.php/AV/article/view/168

Bashir, B., y Khalique, A. (2016). *Una revisión sobre seguridad versus ética. Revista Internacional de Aplicaciones Informáticas*, 151(11), 244-249.

Besares, A. (2015). *Tópicos de Derecho Informático*. Texas: UNACH https://www.iijunach.mx/images/publicaciones/Topicos_de_Derecho_Informatico.pdf

Blossiers, J. (2018). *El delito informático y su incidencia en la empresa bancaria.* [Tesis de Maestría, Universidad Nacional Federico Villarreal]. http://repositorio.unfv.edu.pe/handle/UNFV/2608

Correa, P. (2016). *Derecho Constitucional General*. Universidad Católica los Ángeles de Chimbote. UTEX. 1° edición. http://repositorio.uladech.edu.pe/handle/ULADECH_CATOLICA/77

García, V. (1999). Teoría del Estado y Derecho Constitucional, 1° ed. Lima: Fondo de Desarrollo Editorial U de L.

Herrera, D. (1987). Derecho Constitucional e Instituciones Políticas, 2° ed. Lima, EDDILI.

La Defensoría de la Niñez (2017). ¿Qué se entiende por vulneración de Derechos? Blog. https://www.defensorianinez.cl/preguntas_frecuentes/que-se-entiende-por-vulneracion-de-derechos

Loredo, J. A., y Ramírez, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Celerinet. 44-51.

http://eprints.uanl.mx/id/eprint/3536

Naciones Unidas (2013). *Estudio exhaustivo sobre el delito cibernético*. Oficina de las Naciones Unidas Contra la Droga y el Delito. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018* [Tesis de posgrado, Universidad Cesar Vallejo] https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Ramírez, D. A., y Castro, E. F. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia.* [Tesis de posgrado, Universidad Nacional Abierta y a Distancia "UNAD"] https://repository.unad.edu.co/handle/10596/17370

Sagüés, N. (2001), *Elementos de Derecho Constitucional*, 3° ed. Buenos Aires: Ed. Astrea.

Téllez, J. (2012). *Delitos Cibernéticos*. Universidad Autónoma de México. file:///C:/Users/Miguel/Downloads/Dialnet-DelitosCiberneticos-248139.pdf

Vásquez, E., Regalado, M., y Guadron, S. (2017). *Cibercrimen e informática forense: introducción y análisis en El Salvador*. Revista Tecnológica; Nº. 10. 63-68. http://www.redicces.org.sv/jspui/bitstream/10972/3029/1/Articulo11.pdf

Villavicencio Terreros, F. (2014). *Delitos Informáticos*. IUS ET VERITAS, 24(49), 284-304. http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Chávez, E. (2018). "El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de

lima norte, 2017". [Tesis para optar el grado académico de Doctor en Derecho]. Universidad Nacional Federico Villareal, Lima. http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=

Espinoza, M. (2017). "Derecho penal informático: deslegitimación del Poder punitivo en la sociedad de control". [Tesis para optar Título de Abogado]. Universidad Nacional del Antiplano, Puno. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza_Coila_Michael.pdf?sequence=1&isAllowed=y

Pardo, A. (2018). "Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018". [Tesis para optar el grado académico de Maestro en Derecho Penal y Procesal Penal]. Universidad Cesar Vallejo, Lima. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Rivera, A. (2017). "La vulneración de los derechos laborales por parte tribunal constitucional en aplicación del precedente vinculante del expediente n° 5057-2013-aa/tc-caso Huatuco". [Tesis para optar el Título profesional de Abogado]. Universidad Ricardo Palma, Lima. https://repositorio.urp.edu.pe/bitstream/handle/urp/1122/TESIS-%20Angie%20Rivera.pdf?sequence=1&isAllowed=y

Romero, M. (2017). "Delitos informáticos cometidos a través de redes sociales y su tratamiento en el Ministerio Publico en la Ciudad de Huánuco, 2016". [Tesis para optar el título profesional de Abogado]. Universidad de Huánuco, Perú. http://repositorio.udh.edu.pe/bitstream/handle/123456789/331/T_047_%2025858529_T.pdf?sequence=1&isAllowed=y

López, J. y Sáenz, M. (2018). "La obtención de la Prueba Penal Internacional en Materia de Delitos Cibernéticos". [Tesis para optar Título de Abogado]. Universidad Politécnico Gran Colombiano, Bogotá.

https://alejandria.poligran.edu.co/bitstream/handle/10823/1501/Ciberdelitos%20%28Monica%20Saenz%20-%20Jessica%20Lopez%29-Ultima%20version%20corregida.pdf?sequence=1&isAllowed=y

Velasco, G. (2019). “Guía operativa para la protección de datos informáticos en empresas mexicanas”. [Tesis para optar Licenciatura]. Universidad Autónoma del estado de México, Texcoco. http://ri.uaemex.mx/bitstream/handle/20.500.11799/100025/TESINA.%20GU%c3%8dA%20OPERATIVA%20PARA%20LA%20PROTECCI%c3%93N%20DE%20DATOS%20INFORMATICOS%20EN%20EMPRESAS%20MEXICANAS.pdf?sequence=1&isAllowed=y

Vaca, M. (2017). “El hacker como sujeto activo el delito: límites y excepciones de la intromisión tecnológica a la red de internet a la luz del código orgánico integral penal (COIP)”. [Tesis para optar título de abogada]. Universidad Católica del Ecuador, Quito. https://www.google.com/search?q=CORCHETES&oq=COR&aqs=chrome.0.69i59j69i57j35i39j0i131i395i433l2j0i395i433j0i131i395i433j69i60.2950j1j7&sourceid=chrome&ie=UTF-8

MATRIZ DE CONSITENCIA

TÍTULO: "Delitos Cibernéticos y Confidencialidad en las Redes Sociales, Ica - 2020"

PROBLEMA	OBJETIVOS	ELEMENTOS DE INVESTIGACION Conocimientos sobre delitos cibernéticos y confidencialidad en las redes sociales de Jueces del cercado de Ica	
		Categorías	Subcategorías
¿De qué manera los delitos cibernéticos se relacionan con la vulneración de confidencialidad en las Redes Sociales?	**Objetivos** **Objetivo General** Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales **Objetivos específicos** Analizar de qué manera el Phishing influye en la interceptación de datos personales	Delitos Cibernéticos	• Phishing • Interceptación de datos personales.
		Ciberdelincuencia en Redes Sociales	• Extorción • Filtración de conversaciones.

	De qué manera la extorción incide en la filtración de conversaciones		
TIPO Y DISEÑO DE INVESTIGACIÓN	**POBLACIÓN Y MUESTRA**	**TÉCNICAS Y ÁMBITO**	**ANÁLISIS DE DATOS**
Enfoque Cualitativo DISEÑO: Teoría fundamentada	POBLACIÓN: La población está constituida por jueces que laboran en el Cercado de Ica Muestra: 3 jueces del Poder Judicial	Técnica: Entrevista semiestructurada Instrumento: guía de entrevista y guía de análisis documental. Ámbito de Aplicación: Institución Poder Judicial del cercado de Ica	Análisis de las entrevistas y la revisión de la bibliografía especializada. Análisis de las experiencias de jueces del Poder Judicial

MATRIZ DE CATEGORIZACIÓN

CAMPO TEMATICO	CATEGORIAS	SUBCATEGORIAS	FRASES FRECUENTES.
Delitos Cibernéticos y Confidencialidad en las Redes Sociales	**Delitos Cibernéticos**	Phishing	Mecanismo de difícil detección
			Contribuye a la captación de datos
			Aumento acelerado de este tipo de delitos
			Originado por mayor acceso a tecnología
			Se destaca la clonación de tarjeta, extorsión, fraude, identidades falsas en redes sociales.
		Interceptación de datos personales.	Origen en la poca seguridad
			Excesiva confianza que se proporciona a extraños
			Falta de información sobre páginas falsas
	Ciberdelincuencia en Redes Sociales	Extorción	Reconoce el fácil acceso a la información privada
			Más frecuente en personas de escasos recursos
		Filtración de conversaciones	Aumento de agentes distractores en plataformas virtuales

Uso inadecuado de la información confidencial y privada de usuarios

VALIDACIÓN DEL INSTRUMENTO GUIA DE ENTREVISTA

VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres: GAMARRA RAMON JOSE CARLOS

1.2 Cargo e institución donde labora: UCV

1.3 Nombre del instrumento motivo de evaluación: Guía de entrevista

1.4 Autora del Instrumento:

II. ASPECTOS DE VALIDACIÓN

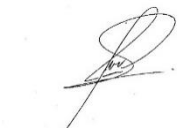
CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Está adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Está adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su												X	

	adecuación al Método Científico.													

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación	X
- El Instrumento no cumple con Los requisitos para su aplicación	

PROMEDIO DE VALORACIÓN: 95%

Lima,  18 de junio del 2021

FIRMA DEL EXPERTO INFORMANTE

DNI N 09919088 Telf.: 963347510

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

VALIDACIÓN DEL INSTRUMENTO

IV. DATOS GENERALES

1.4 Apellidos y Nombres: LUCA ACETO

1.5 Cargo e institución donde labora: UCV

1.6 Nombre del instrumento motivo de evaluación: Guía de entrevista

1.4 Autora del Instrumento:

V. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Está adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Está adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

VI. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación	X
- El Instrumento no cumple con Los requisitos para su aplicación	
PROMEDIO DE VALORACIÓN:	95%

Lima, 18 de junio del 2021

FIRMA DEL EXPERTO INFORMANTE

DNI N 48974953 Telf.: 910190409

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Dr. Mogollón Longa Johnny William

1.2. Cargo e institución donde labora: Docente de la Escuela de Derecho de la UCV

1.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista

1.4. Autor(A) de Instrumento:

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.													x
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.													x
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.													x
4. ORGANIZACIÓN	Existe una organización lógica.													x
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales													x
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.													x
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.													x
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos													x
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.													x
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la												x	

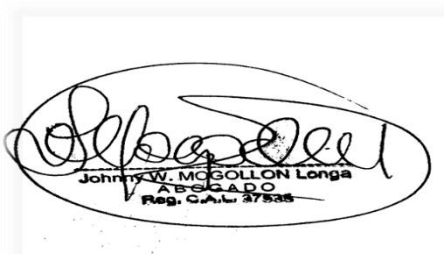
	investigación y su adecuación al Método Científico.													

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación	X
- El Instrumento no cumple con Los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN: 99%

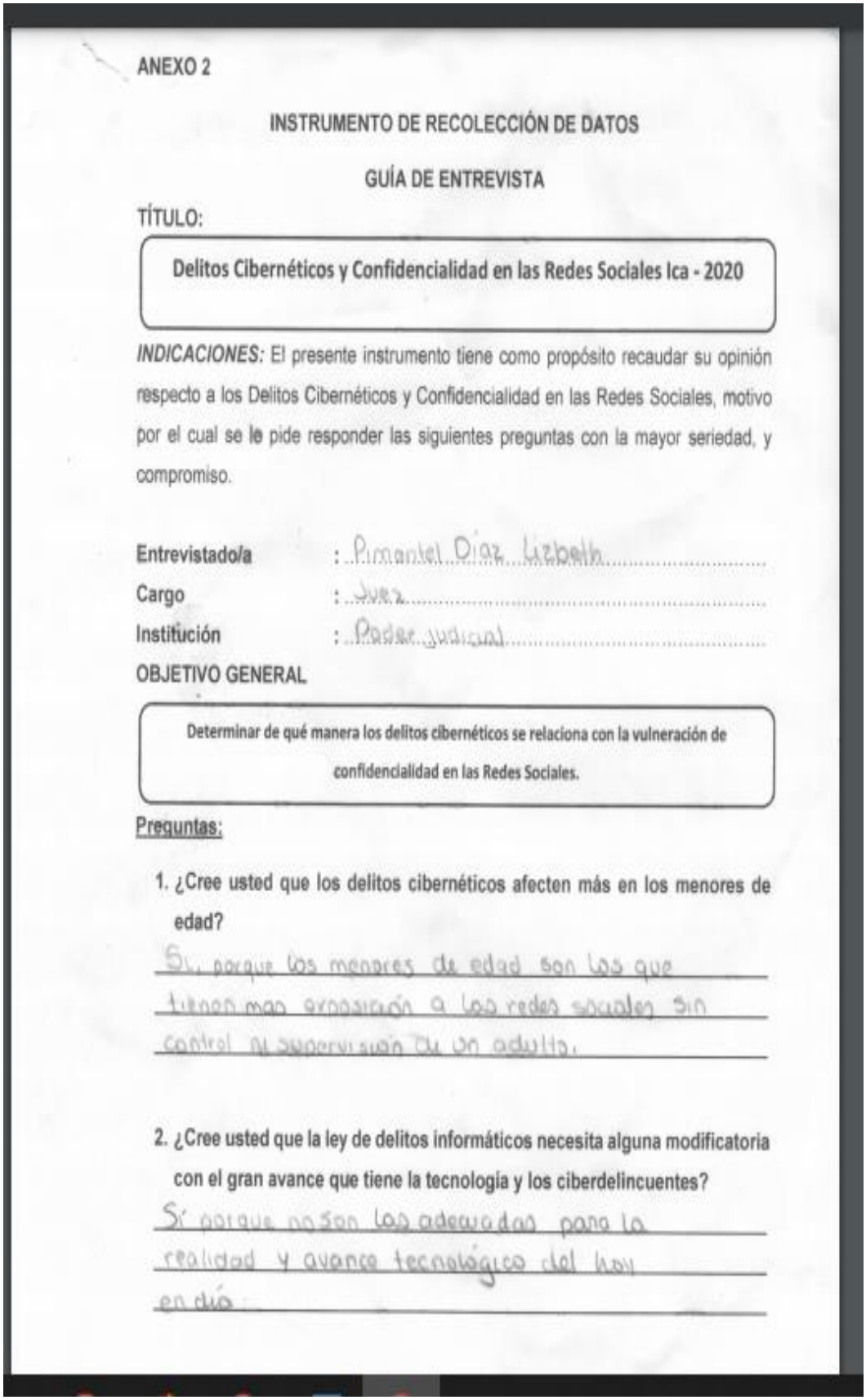
Lima, 1 Julio del 2021



FIRMA DEL EXPERTO INFORMANTE

DNI N° 43329698 Telf.:

GUIA DE ENTREVISTA



ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

TÍTULO:

Delitos Cibernéticos y Confidencialidad en las Redes Sociales Ica - 2020

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto a los Delitos Cibernéticos y Confidencialidad en las Redes Sociales, motivo por el cual se le pide responder las siguientes preguntas con la mayor seriedad, y compromiso.

Entrevistado/a : Pimentel Diaz Lizbeth

Cargo : Juez

Institución : Poder judicial

OBJETIVO GENERAL

Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales.

Preguntas:

1. ¿Cree usted que los delitos cibernéticos afecten más en los menores de edad?

Si, porque los menores de edad son los que tienen mas exposición a las redes sociales sin control ni supervisión de un adulto.

2. ¿Cree usted que la ley de delitos informáticos necesita alguna modificatoria con el gran avance que tiene la tecnología y los ciberdelincuentes?

Si porque no son los adecuados para la realidad y avance tecnológico del hoy en día

3. De acuerdo con usted, ¿De qué forma afectan los delitos cibernéticos?

Afectan considerablemente a la población niños- adolescentes con el tema de estafas prostitución, pornografía, entre otras.

OBJETIVO ESPECÍFICO 1

Analizar de qué manera el Phishing influye en la interceptación de datos personales

Preguntas:

4. ¿Considera Ud. que el uso del el Phishing influye en la interceptación de datos personales?

Sí porque es un mecanismo muy difícil de detectar.

5. Según su experiencia profesional, ¿Cuál considera que son los factores que se determinan sobre el uso del Phishing en la interceptación de datos personales?

El principal factor es la falta de información.

6. ¿Cree usted que en los últimos años se ha incrementado los casos de phishing

Sí, así como a avanzado la tecnología que hace que los menores de edad entren a páginas web sin supervisión.

OBJETIVO ESPECÍFICO 2

De qué manera la extorción incide en la filtración de conversaciones

Preguntas:

7. ¿Cree usted que las extorciones del hoy en día son producto a la filtración de conversaciones?

Si, hoy en dia han llegado una gran cantidad de denuncias referente al tema de extorcion por filtración de conversaciones

8. ¿Usted considera que la extorción cibernética debería tener una condena drástica?

Si, por eso es que lo siguen haciendo porque no hay condenas drásticas

9. ¿Según su experiencia profesional, ¿Cuál considera que es el modus operandi de los ciberdelincuentes en la Región de Ica?

Identidades falsas en las redes sociales asi como tambien asi como tambien los numeros telefonicos

SELLO	FIRMA
	Lizbeth

ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

TÍTULO:

Delitos Cibernéticos y Confidencialidad en las Redes Sociales Ica - 2020

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto a los Delitos Cibernéticos y Confidencialidad en las Redes Sociales, motivo por el cual se le pide responder las siguientes preguntas con la mayor seriedad, y compromiso.

Entrevistado/a : Gina Mariño Calderón.

Cargo : Secretaria judicial.

Institución : Poder Judicial.

OBJETIVO GENERAL

Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales.

Preguntas:

1. **¿Cree usted que los delitos cibernéticos afecten más en los menores de edad?**

Si. Porque los menores de edad son usuarios constantes de los redes sociales y son vulnerables a delitos por medios cibernéticos.

2. **¿Cree usted que la ley de delitos informáticos necesita alguna modificatoria con el gran avance que tiene la tecnología y los ciberdelincuentes?**

Desde mi punto de vista la ley vigente necesita una modificatoria inmediata, ya que no se adecua a la realidad siendo ineficaz.

3. De acuerdo con usted, ¿De qué forma afectan los delitos cibernéticos?

Considero que afecta gravemente a la integridad de un sector vital de la sociedad.

OBJETIVO ESPECÍFICO 1

Analizar de qué manera el Phishing influye en la interceptación de datos personales

Preguntas:

4. ¿Considera Ud. que el uso del el Phishing influye en la interceptación de datos personales?

Desde mi punto de vista, hasta cierto punto ya que es una herramienta limitada.

5. Según su experiencia profesional, ¿Cuál considera que son los factores que se determinan sobre el uso del Phishing en la interceptación de datos personales?

La poca seguridad virtual, debido al pésimo labor del estado en el control de los datos.

6. ¿Cree usted que en los últimos años se ha incrementado los casos de phishing

Considero que sí, ya que este conocimiento se ha expandido.

OBJETIVO ESPECÍFICO 2

De qué manera la extorción incide en la filtración de conversaciones

Preguntas:

7. ¿Cree usted que las extorciones del hoy en día son producto a la filtración de conversaciones?

Si, ya que son materiales grabados con información que se pueden convertir en extorción

8. ¿Usted considera que la extorción cibernética debería tener una condena drástica?

Debe tener una pena mayor a la extorción normal.

9. ¿Según su experiencia profesional, ¿Cuál considera que es el modus operandi de los ciberdelincuentes en la Región de Ica?

Mel Phishing.

SELLO	FIRMA

ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

TÍTULO:

Delitos Cibernéticos y Confidencialidad en las Redes Sociales Ica - 2020

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto a los Delitos Cibernéticos y Confidencialidad en las Redes Sociales, motivo por el cual se le pide responder las siguientes preguntas con la mayor seriedad, y compromiso.

Entrevistado/a : Luzmila V. Echegaray Bernedo

Cargo : Especialista Judicial

Institución : Poder Judicial

OBJETIVO GENERAL

Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales.

Preguntas:

1. **¿Cree usted que los delitos cibernéticos afecten más en los menores de edad?**

Si, porque a través de ello muchas personas engañan a los menores que son vulnerables por su edad.

2. **¿Cree usted que la ley de delitos informáticos necesita alguna modificatoria con el gran avance que tiene la tecnología y los ciberdelincuentes?**

Si, porque debería haber una ley que prohiba ciertas páginas que pueden ingresar los menores y pena más drásticas para los personas que los engañen.

3. De acuerdo con usted, ¿De qué forma afectan los delitos cibernéticos?

Si afectan, porque muchas veces a través de ello a muchas personas, a través de su vulnerabilidad, además a las personas que obtienen de esta misma manera los ingresos y no son donen Tarjetas.

OBJETIVO ESPECÍFICO 1

Analizar de qué manera el Phishing influye en la interceptación de datos personales

Preguntas:

4. ¿Considera Ud. que el uso del el Phishing influye en la interceptación de datos personales?

No. Conozco Sobre el Phishing.

5. Según su experiencia profesional, ¿Cuál considera que son los factores que se determinan sobre el uso del Phishing en la interceptación de datos personales?

6. ¿Cree usted que en los últimos años se ha incrementado los casos de phishing

OBJETIVO ESPECÍFICO 2

De qué manera la extorción incide en la filtración de conversaciones

Preguntas:

7. ¿Cree usted que las extorciones del hoy en día son producto a la filtración de conversaciones?

No siempre, porque muchas veces también es información a favor ventaja.

8. ¿Usted considera que la extorción cibernética debería tener una condena drástica?

Si, para un gio través de ello la gente tenga más cuidado. y no cometan delito.

9. ¿Según su experiencia profesional, ¿Cuál considera que es el modus operandi de los ciberdelincuentes en la Región de Ica?

Bueno a mi criterio y experiencia creo que es la clonación de Tarjetas.

SELLO	FIRMA
no Tengo Sello	

ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

TÍTULO:

Delitos Cibernéticos y Confidencialidad en las Redes Sociales Ica - 2020

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto a los Delitos Cibernéticos y Confidencialidad en las Redes Sociales, motivo por el cual se le pide responder las siguientes preguntas con la mayor seriedad, y compromiso.

Entrevistado/a : Diana Ventura Calderon

Cargo : .....

Institución : .....

OBJETIVO GENERAL

Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales.

Preguntas:

1. ¿Cree usted que los delitos cibernéticos afecten más en los menores de edad?

Si los afecta ya que no tienen demasiada experiencia usando redes y el tipo mayor de delitos cibernéticos es mucho más facil y común.

2. ¿Cree usted que la ley de delitos informáticos necesita alguna modificatoria con el gran avance que tiene la tecnología y los ciberdelincuentes?

Si la ley no esta hecha con piedra, las leyes cambian con el paso del tiempo y con la tecnología que se va perfeccionando y con ello los delitos mejoran.

3. De acuerdo con usted, ¿De qué forma afectan los delitos cibernéticos?

Vulneran la privacidad de las personas y exponen a sufrir dichos delitos, infringen los Terminos de privacidad y seguridad de algunas páginas Web.

OBJETIVO ESPECÍFICO 1

Analizar de qué manera el Phishing influye en la interceptación de datos personales

Preguntas:

4. ¿Considera Ud. que el uso del el Phishing influye en la interceptación de datos personales?

Si, porque somos conscientes de la realidad sobre los datos personales al hacerlo pasan por algunos.

5. Según su experiencia profesional, ¿Cuál considera que son los factores que se determinan sobre el uso del Phishing en la interceptación de datos personales?

Uno de los factores importantes creo que es la inocencia y confianza que tiene la victima al sufrir dicho delito.

6. ¿Cree usted que en los últimos años se ha incrementado los casos de phishing

Creo que si, en los ultimos años ha incrementado al ver que los ciudadanos tienen un mayor acceso a la Tecnología.

OBJETIVO ESPECÍFICO 2

De qué manera la extorción incide en la filtración de conversaciones

Preguntas:

7. ¿Cree usted que las extorciones del hoy en día son producto a la filtración de conversaciones?

Si, para que algun extorsionador debe Tener una información importante de dicha Victima para cometer el delito

8. ¿Usted considera que la extorción cibernética debería tener una condena drástica?

No Tan drastica, ya que puede ser o a depender de la gravedad del hecho.

9. ¿Según su experiencia profesional, ¿Cuál considera que es el modus operandi de los ciberdelincuentes en la Región de Ica?

Según mi experiencia creo que la modalidad es que buscan a Victimas de las zonas de bajos recursos donde desconocen estas modalidades de estafas y así cometer el delito de información,

SELLO	FIRMA

ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA

TÍTULO:

Delitos Cibernéticos y Confidencialidad en las Redes Sociales Ica - 2020

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto a los Delitos Cibernéticos y Confidencialidad en las Redes Sociales, motivo por el cual se le pide responder las siguientes preguntas con la mayor seriedad, y compromiso.

Entrevistado/a : Sandra Fernandez Valencia

Cargo : Asistente

Institución : Poder Judicial

OBJETIVO GENERAL

Determinar de qué manera los delitos cibernéticos se relaciona con la vulneración de confidencialidad en las Redes Sociales.

Preguntas:

1. **¿Cree usted que los delitos cibernéticos afecten más en los menores de edad?**

Si Creo porque los menores de edad no estan concientes de los peligros que impliquen exponerse en la Web.

2. **¿Cree usted que la ley de delitos informáticos necesita alguna modificatoria con el gran avance que tiene la tecnologia y los ciberdelincuentes?**

Si necesitan de modificatorias de acuerdo a la tecnologia que avanza.

3. De acuerdo con usted, ¿De qué forma afectan los delitos cibernéticos?

Afecta directamente a la intimidad de documentos, conversaciones, secretos de las personas naturales y jurídicas.

OBJETIVO ESPECÍFICO 1

Analizar de qué manera el Phishing influye en la interceptación de datos personales

Preguntas:

4. ¿Considera Ud. que el uso del el Phishing influye en la interceptación de datos personales?

Si influye ya que el Phishing es el delito de engañar a las personas para que compartan información confidencial.

5. Según su experiencia profesional, ¿Cuál considera que son los factores que se determinan sobre el uso del Phishing en la interceptación de datos personales?

la confianza que le pueden dar hacia la otra persona. y de esta manera engañan y logran que le puedan dar su información personal.

6. ¿Cree usted que en los últimos años se ha incrementado los casos de phishing

Si se ha incrementado por el acceso a la tecnología.

OBJETIVO ESPECÍFICO 2

De qué manera la extorción incide en la filtración de conversaciones

Preguntas:

7. ¿Cree usted que las extorciones del hoy en día son producto a la filtración de conversaciones?

Si Son producto a la filtración porque los extorcionadores deben Tener una información importante Sobre su privacidad del Usuario.

8. ¿Usted considera que la extorción cibernética debería tener una condena drástica?

Debería Ser de acuerdo al hecho (Gravedad).

9. ¿Según su experiencia profesional, ¿Cuál considera que es el modus operandi de los ciberdelincuentes en la Región de Ica?

Según mi experiencia profesional Considero la extorsión el fraude.

SELLO	FIRMA