

UNIVERSIDAD PERUANA DE LAS AMÉRICAS



ESCUELA DE DERECHO

TESIS

**“La influencia de los delitos informáticos en el crimen
organizado en el distrito de San Isidro-2020”**

PARA OPTAR EL TÍTULO DE ABOGADO.

AUTOR:

LOURDES MAXIMINA HUARCAYA BORDA

(ORCID: 0000-0003-3269-1072)

ASESOR:

Mg. MARTIN MORALES GALLO

(ORCID: 0000-0002-1471-8983)

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO.

LIMA, PERÚ.

FEBRERO, 2021.

Dedicatoria

A mi amada MADRE, a quien le debo todo lo que soy, por su apoyo incondicional. Y a mi amado PADRE quien fue mi inspiración y motivación principal, que me brindó todo su apoyo en el transcurso de mi Carrera Profesional, un sueño hecho realidad. Siempre serás el faro que guía mi camino, mi vida y ejemplo de lucha constante, así como el amor que brindas a tu familia que traspasa la eternidad.

Agradecimientos

A mis padres y hermanos por su amor inconmensurable. A mi esposo por su constante comprensión y ternura.

A mi universidad, MI ALMA MATER y su equipo de trabajo por su constante guía y aportes. Y muy especialmente a mi asesora de tesis Silvia Salazar Llerena, con gratitud y cariño

Resumen

El trabajo de investigación presente tiene como objetivo determinar la influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro – 2020.

Los delitos informáticos según (Chávez Rodríguez, 2018) son aquellos comportamientos con los cuales se busca desestabilizar los sistemas de dispositivos de seguridad, dígase, invasión a computadores, correos o sistema de datos que requieren una contraseña de acceso, las cuales son conductas que pueden ser llevadas a cabo únicamente con el uso de la tecnología. Lo que se busca es comprender como esta clase de delitos ha impactado en las organizaciones criminales y el crimen organizado, pues esta relación es clave para poder llevar a cabo estrategias que permitan frenar su actuar delictivo. El crimen organizado y las organizaciones criminales son según el (Congreso de la República del Perú, 2013) cualquier conjunto de tres o más personas los cuales se dividen diferentes roles, e independientemente de su estructura y su campo de acción, se crea, funciona o existe de manera indefinida en el tiempo con el objetivo de cometer una o más conductas criminales graves señaladas en el artículo 3 de la ley 30077. La presente investigación se centra en las dimensiones de conductas maliciosas, crimen electrónico, jerarquía estructurada y transnacionalidad, las cuales son importantes para entender la relación que existe entre los delitos informáticos y el crimen organizado.

La presente es una investigación aplicada no experimental transeccional correlacional, que se realizó bajo el enfoque cuantitativo aplicando la técnica de la encuesta en 50 personas que laboran o visitan la comisaria de San Isidro.

Palabras clave:

Delito informático, Crimen organizado, Conductas maliciosas, Organizaciones criminales

Abstract

The present research work aims to determine the influence of computer crimes within organized crime in the district of San Isidro - 2020.

Computer crimes according to (Chávez Rodríguez, 2018) are those behaviors that seek to destabilize the security device systems, say, invasion of computers, post office or data system that require an access password, which are behaviors that can be carried out solely with the use of technology. What is sought is to understand how this type of crime has impacted criminal organizations and organized crime, as this relationship is key to be able to carry out strategies that allow stopping their criminal behavior. Organized crime and criminal organizations are according to the (Congress of the Republic of Peru, 2013) any group of three or more people who divide different roles, which regardless of their structure and their field of action, is created, works or it exists indefinitely in time with the aim of committing one or more serious criminal conducts indicated in article 3 of Law 30077. This investigation focuses on the dimensions of malicious conduct, electronic crime, structured hierarchy and transnationality, which are important to understand the relationship between cybercrime and organized crime.

This is a non-experimental correlational transectional applied research, which was carried out under the quantitative approach, applying the survey technique in 50 people who work or visit the San Isidro police station.

Keywords:

Cybercrime, Organized Crime, Malicious Behavior, Criminal Organizations

Tabla de contenidos

Dedicatoria	ii
Agradecimientos	iii
Resumen	iv
Abstract	v
Tabla de contenidos	vi
Lista de Tablas	xii
Lista de Figuras	xiv
Introducción	1
Capítulo I: Problema de la Investigación	3
1.1 Descripción de la Realidad Problemática	3
1.2 Planteamiento del Problema	4
1.2.1. Problema General.	4
1.2.2. Problemas Específicos.	4
1.3 Objetivos de la Investigación	4
1.3.1. Objetivo General.	4
1.3.2. Objetivos Específicos.	4
1.4 Justificación e Importancia de la Investigación	5
1.4.1. Justificación	5
1.4.2. Importancia	5

1.5	Limitaciones de la Investigación	6
Capítulo II: Marco Teórico		7
2.1	Antecedentes de la Investigación	7
2.1.1.	Internacionales.	7
2.1.2.	Nacionales	11
2.2	Bases teóricas	16
2.2.1.	Bases Teóricas sobre Delitos Informáticos	16
2.2.1.1.	La Teoría del Delito	16
2.2.1.2.	Concepto de delitos informáticos y delitos electrónicos	17
2.2.1.3.	Las posibles relaciones, la acción dolosa y la acción culposa	17
2.2.1.4.	El delito informático en el código Penal Peruano: art. 186° - A	17
2.2.1.5.	Descripción típica y modalidades de los delitos informáticos	18
2.2.1.6.	Delitos informáticos tipificados en el Ordenamiento Jurídico peruano	18
2.2.2.	Bases teóricas de Crimen Organizado:	20
2.2.2.1.	Concepto	20
2.2.2.2.	Naturaleza jurídica del crimen organizado	20
2.2.2.3.	Características del crimen organizado	21
2.2.2.3.1.	Líneas distintivas de la criminalidad organizada y diferencias con la banda criminal	21
2.2.2.3.2.	Características propias de la criminalidad organizada	21

2.2.2.4.	Objetivos de las organizaciones criminales	22
2.2.2.5.	Formas de organización criminal	22
2.2.2.5.1.	Etapa Predatoria	22
2.2.2.5.2.	Etapa Parasitaria	23
2.2.2.5.3.	Etapa simbiótica	24
2.2.2.6.	El crimen organizado transnacional	24
2.3	Definición de Términos Básicos	24
2.3.1.	Delitos Informáticos	24
2.3.1.1.	Conductas Maliciosas	25
2.3.1.1.1.	Necesidad de modernizar leyes	26
2.3.1.1.2.	Explotación de datos personales	27
2.3.1.2.	Crimen Electrónico	28
2.3.1.2.1.	Estafa	29
2.3.1.2.2.	Beneficio ilícito	30
2.3.2.	Crimen Organizado	31
2.3.2.1.	Jerarquía estructurada	32
2.3.2.1.1.	Intervención delictiva	33
2.3.2.1.2.	Planificación	34
2.3.2.2.	Transnacionalidad	35
2.3.2.2.1.	Extorsiones Delictivas	36

2.3.2.2.2. Grupos criminales	37
Capítulo III: Marco Metodológico	39
3.1 Enfoque de la Investigación	39
3.2 Variables	39
3.2.1. Operacionalización de variables.	39
3.2.1.1. Variable independiente (X-1).	39
3.2.1.1.1. Dimensiones	39
3.2.1.1.2. Indicadores.	39
3.2.1.2. Variable dependiente (Y-2).	40
3.2.1.2.1. Dimensiones	40
3.2.1.2.2. Indicadores.	40
3.3 Hipótesis	41
1.3.1. Hipótesis General.	41
1.3.2. Hipótesis Específicas.	41
3.4 Tipo de Investigación	42
3.5 Diseño de la investigación	42
3.6 Población y Muestra	42
3.6.1. Población.	42
3.6.1.1. Criterios de inclusión.	42
3.6.1.2. Criterios de exclusión.	42

	x
3.6.2. Muestra.	43
3.7 Técnicas e Instrumentos de Recolección de Datos	43
3.7.1. Técnica.	43
3.7.2. Instrumento de recolección de datos.	43
3.7.2.1. Análisis de fiabilidad del instrumento	43
3.7.2.2. Validez del instrumento	44
Capítulo IV: Resultados	45
4.1 Análisis de los Resultados	45
4.1.1. Distribución de frecuencia.	45
4.1.2. Correlación.	63
4.1.2.1. Prueba de hipótesis general.	63
4.1.2.2. Prueba de hipótesis específicas.	64
4.2 Discusión	68
Conclusiones:	70
Recomendaciones:	72
Referencias:	74
Anexo N° 01: Matriz de consistencia	82
Anexo N° 02: Instrumento de la Investigación	84
Anexo N° 03: Instrumento de Validación	86
Anexo N° 04: Ejemplo de campaña para evitar ser víctima de la delincuencia informática.	88

Anexo N° 05: Extorsión por Estafa Romántica	89
Anexo N° 06: Extorsión sexual	90
Anexo N° 06: correos de extorsión dirigidos a empresas	93
Anexo N° 07: Resolución legislativa N° 30913	94
Anexo N° 08: Fragmento del convenio de Budapest	95

Lista de Tablas

Tabla 1	21
Tabla 2	24
Tabla 3	25
Tabla 4	26
Tabla 5	27
Tabla 6	28
Tabla 7	29
Tabla 8	30
Tabla 9	31
Tabla 10	32
Tabla 11	33
Tabla 12	34
Tabla 13	35
Tabla 14	36
Tabla 15	37
Tabla 16	38
Tabla 17	39
Tabla 18	40
Tabla 19	41
Tabla 20	42
Tabla 21	43
Tabla 22	44

Tabla 23

45

Tabla 24

46

Lista de Figuras

Figura 1: Delitos Informáticos	19
Figura 2: Conductas Maliciosas	20
Figura 3: Crimen Electrónico	21
Figura 4: Crimen Organizado	22
Figura 5: Jerarquía Estructurada	23
Figura 6: Transnacionalidad	24
Figura 7: Gráfico de barras de la Pregunta 01. ¿Considera usted que es necesario modernizar las leyes debido a que con el paso del tiempo aparecen nuevos delitos? Fuente: Elaboración propia – SPSS	31
Figura 8: Gráfico de barras de la Pregunta 02: ¿Está usted de acuerdo en que se deben incorporar más leyes para regular los delitos informáticos? Fuente: Elaboración propia – SPSS	32
Figura 9: Gráfico de barras de la Pregunta 03: ¿Cree usted que la explotación de datos personales que se da debido a los delitos informáticos constituye una grave falta a la integridad de la persona? Fuente: Elaboración propia – SPSS	33
Figura 10: Gráfico de barras de la Pregunta 04: ¿Piensa usted que la explotación de datos personales ocurre porque muchas personas no tienen el conocimiento adecuado sobre los hackers? Fuente: Elaboración propia – SPSS	34
Figura 11: Gráfico de barras de la Pregunta 05: ¿Considera usted que el principal objetivo de los delitos informáticos es la estafa? Fuente: Elaboración propia – SPSS	35
Figura 12: Gráfico de barras de la Pregunta 06: ¿Está usted de acuerdo en que las principales víctimas de estafa son los adultos mayores? Fuente: Elaboración propia – SPSS	36

- Figura 13: Gráfico de barras de la Pregunta 07 ¿Cree usted que los hackers logran su objetivo obteniendo un beneficio ilícito? Fuente: Elaboración propia – SPSS 37
- Figura 14: Gráfico de barras de la Pregunta 08 ¿Considera usted que el beneficio ilícito es fundamental para que la organización criminal se mantenga con el tiempo? Fuente: Elaboración propia – SPSS 38
- Figura 15: Gráfico de barras de la Pregunta 09. ¿Considera usted que hay baja intervención delictiva respecto al crimen organizado? Fuente: Elaboración propia – SPSS 39
- Figura 16: Gráfico de barras de la Pregunta 10. ¿Está usted de acuerdo en que la intervención delictiva no es justa como se requiere? Fuente: Elaboración propia – SPSS 40
- Figura 17: Gráfico de barras de la Pregunta 11. ¿Cree usted que la planificación y repartición de tareas facilita el actuar criminal de las organizaciones criminales? Fuente: Elaboración propia – SPSS 41
- Figura 18: Gráfico de barras de la Pregunta 12. ¿Piensa usted que la planificación y repartición de tareas influyen en la creación de una identidad dentro de la organización criminal? Fuente: Elaboración propia – SPSS 42
- Figura 19: Gráfico de barras de la Pregunta 13 ¿Considera usted que las extorsiones delictivas se realizan desde cualquier parte o lugar? Fuente: Elaboración propia – SPSS 43
- Figura 20: Gráfico de barras de la Pregunta 14: ¿Cree usted que las extorsiones facilitan la comisión de delitos informáticos? Fuente: Elaboración propia – SPSS 44
- Figura 21: Gráfico de barras de la Pregunta 15. ¿ Está usted de acuerdo en que la valorización de los beneficios ilícitos afecta a la cantidad de integrantes de un grupo criminal? Fuente: Elaboración propia – SPSS 45
- Figura 22: Gráfico de barras de la Pregunta 16. ¿Piensa usted que no se les juzga a los grupos criminales como se debería? Fuente: Elaboración propia – SPSS 46

Introducción

El presente trabajo de investigación tuvo como objetivo general, determinar la influencia de los delitos informáticos dentro del crimen organizado en el distrito de San Isidro – 2020, asimismo se tuvieron los siguientes objetivos específicos: (a) analizar la influencia de la necesidad de modernizar en la intervención delictiva en el distrito de San Isidro- 2020. (b) detallar la influencia de la explotación de datos personales en la planificación de las organizaciones criminales en el distrito de San Isidro- 2020. (c) establecer la influencia de la estafa en las extorsiones delictivas en el distrito de San Isidro- 2020. (d) mencionar la influencia del beneficio ilícito en los grupos criminales en el distrito de San Isidro- 2020; la hipótesis general que se plantea en la investigación es que los delitos informáticos influyen en el crimen organizado en el distrito de San Isidro – 2020; y las hipótesis específicas son: (a) la necesidad de modernizar leyes influye en la intervención delictiva en el distrito de San Isidro- 2020, (b) la explotación de datos personales influye en la planificación de las organizaciones criminales en el distrito de San Isidro- 2020, (c) la estafa influye en las extorsiones delictivas en el distrito de San Isidro- 2020, (d) el beneficio ilícito influye en los grupos criminales en el distrito de San Isidro- 2020.

Se realizó bajo el enfoque cuantitativo, utilizando como técnica la encuesta de opinión con la ayuda de un cuestionario virtual aplicado por internet, conteniendo 16 preguntas cerradas con alternativas tipo Likert referentes a las variables de estudio “delito informático” y “crimen organizado” con el propósito de establecer la relación entre ambas variables procesando los datos recolectados con el Software SPSS v21. Se trató de una investigación aplicada no experimental transeccional correlacional, con una población conformada por personas que laboran o visitan la comisaría de San Isidro, excluyendo a las personas que no laboran o visitan esta comisaría.

Por consiguiente, el trabajo realizado se articula de la siguiente manera:

En el capítulo I, abarcará todo lo relacionado al problema de investigación es por ello que se plantea lo que son los delitos informáticos, se menciona el problema general, problemas específicos, objetivo general y objetivos específicos, de la mano con algunas ideas que refuerzan la investigación y la hacen más viable.

En el capítulo II, se precisarán todos los factores que corresponden al marco teórico. Es por ello que se establece un enfoque en sus antecedentes tanto internacionales como nacionales, que según la doctrina o el código permita formar una noción del tema que se irá abarcando.

Después se vincularán conceptos relacionados a las variables, tales conductas maliciosas, transnacionalidad, jerarquía estructurada, crimen electrónico entre otros términos presentes en la sección denominada definición de términos básicos.

En el capítulo III, se mencionará cual fue la metodología de la investigación, los factores que intervienen, las hipótesis, población, muestra, método de investigación y mecanismos y estrategias de recopilación de datos.

En el capítulo IV, se interpretará respecto al análisis de resultados como se puede confirmar o denegar lo planteado anteriormente en el marco de las hipótesis.

En la sección final del trabajo, se presentarán las conclusiones y recomendaciones para que se pueda sintetizar y concluir todos los detalles mencionados en todo el proceso de la investigación.

Capítulo I: Problema de la Investigación

1.1 Descripción de la Realidad Problemática

En los últimos años, los ciudadanos de Lima y distintas partes del Perú han realizado compras a través de internet, debido a que genera una comodidad, rapidez y facilidad para adquirir un producto o servicio. Por otro lado, existe una variedad de marcas virtuales que mediante las redes sociales o propias páginas webs ofrecen diversos artefactos, productos y servicios en general.

Existen muchas tiendas virtuales, que cuentan con locales físicos, las cuales son marcas reconocidas y generan confianza debido al tiempo que llevan en el rubro comercial que se centran en la garantía de los productos o servicios. Asimismo, también sobresalen nuevas tiendas que ofrecen productos a precios cómodos, sin embargo, no tienen un establecimiento físico, y para muchas personas puede resultar de desconfianza, ya que se ha generado una cantidad de denuncias respecto a estafas, compras fraudulentas y fraudes informáticos.

Otro problema perjudicial es el robo de información, tarjetas de crédito y extorsiones, donde los delincuentes hacen uso de programas especiales para este tipo de acciones, al igual que el de las redes sociales, enviar mensajes de texto a sus víctimas e incluso llegar al acoso sexual y amenazas constante.

Por lo que se propone en esta investigación es verificar cómo influye los delitos informáticos en el crimen organizado en la ubicación de San Isidro.

1.2 Planteamiento del Problema

1.2.1. Problema General.

- ¿Cuál es la influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro -2020?

1.2.2. Problemas Específicos.

- ¿Cómo influye la necesidad de modernizar las leyes en la intervención delictiva del crimen organizado en el distrito de San Isidro - 2020?
- ¿De qué forma la explotación de datos personales influye en la planificación de las organizaciones criminales en el distrito de San Isidro - 2020?
- ¿De qué forma la estafa influye en las extorsiones delictivas transnacionales del crimen organizado en el distrito de San Isidro- 2020?
- ¿Cómo el beneficio ilícito influye en los grupos criminales transnacionales del crimen organizado en el distrito de San Isidro- 2020?

1.3 Objetivos de la Investigación

1.3.1. Objetivo General.

- Determinar la influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro - 2020.

1.3.2. Objetivos Específicos.

- Analizar la influencia de la necesidad de modernizar las leyes en la intervención delictiva del crimen organizado en el distrito de San Isidro- 2020.

- Detallar la influencia de la explotación de datos personales en la planificación de las organizaciones criminales en el distrito de San Isidro - 2020
- Establecer la influencia de la estafa en las extorsiones delictivas transnacionales del crimen organizado en el distrito de San Isidro- 2020.
- Mencionar la influencia del beneficio ilícito en los grupos criminales transnacionales del crimen organizado en el distrito de San Isidro- 2020.

1.4 Justificación e Importancia de la Investigación

1.4.1. Justificación

El trabajo de investigación presente se justifica en la necesidad de saber la influencia que tienen los delitos informáticos en el crimen organizado, así como la necesidad de modernizar su regulación o sanción, el mal uso de los datos personales, nuevas formas de estafa y el beneficio ilícito que generan, en la intervención delictiva y planificación de las organizaciones criminales, y las nuevas formas de extorsión y grupos criminales transnacionales, para así prevenir que más personas sean víctimas de los hackers o personas que quieren poner en riesgo su información personal o sacar beneficio de algo que no es legal. Comprende una justificación teórica puesto que genera una reflexión; asimismo, se justifica en la práctica, pues su desarrollo ayudará a conocer la influencia existente que tienen los delitos informáticos en el crimen organizado en el distrito de San Isidro en el 2020.

1.4.2. Importancia

La importancia de este trabajo es que servirá de punto de partida para las demás personas que se encuentren investigando sobre la influencia de los delitos informáticos con respecto al

crimen organizado en una comisaría. Servirá, asimismo de guía o apoyo para futuras investigaciones que deseen realizar proyectos con un enfoque similar.

1.5 Limitaciones de la Investigación

La limitación principal de la investigación fue la pandemia mundial ocasionada por el COVID-19 y el Estado de Emergencia decretado en el Perú, el cual afectó de manera notable el llevar a cabo ciertos métodos de recolección de datos, lo cual demoró la entrega de la investigación respecto al plazo establecido inicialmente.

Otra limitación fue con respecto al aspecto económico, ya que además del alto costo que lleva realizar una investigación como esta, la situación actual en consecuencia del Coronavirus originó que el dinero que estaba destinado para la misma tuviera que ser destinado para cubrir gastos que no estaban previstos en primera instancia.

Capítulo II: Marco Teórico

2.1 Antecedentes de la Investigación

2.1.1. Internacionales.

El autor en su tesis “Crimen Organizado Corporativo” considera que la comunicación es el factor más importante dentro una organización criminal ya que la comunicación permite que se den acciones encaminadas a estimular o motivar a los integrantes a cometer delitos, además que permite que se construya una identidad de colectivo lo que genera que se anulen las voluntades individuales y se logre un vínculo total entre las metas personales y las metas de la organización (Carranza Figón, 2017).

En mi opinión, la comunicación siempre va a estar en un plan de ejecución criminal debido a que, se tienen que informar la tarea que cada integrante cometerá y como intervendrán al momento de cometer dicho acto ilícito, es por ello que sin la comunicación no podrían enterarse del rol que cada quién desempeñara.

Martínez (2015) en su tesis “Estrategias multidisciplinarias de seguridad para prevenir el crimen organizado” explica que la información que permite investigar organizaciones de crimen organizado son las víctimas, los delincuentes que se arrepienten y técnicas de investigación tales como el agente encubierto, las entregas vigiladas y la vigilancia con tecnología. Manifiesta también que las fuentes de información que dan mejores resultados son la vigilancia con tecnología, las entregas vigiladas y el agente encubierto debido a que las otras medidas no tienen garantías legales que fomenten su ejecución.

En mi opinión, para que puedan descubrir los planes de una organización criminal se da solo si captan a uno de los sujetos que pertenece a la organización y este por querer salvarse testifica, llegando así a descubrir todos los movimientos y acciones que realizaron; otra manera de descubrirlos es bajo una estrategia del agente encubierto que muchas veces funciona debido a que en nuestro país para captar a estas organizaciones recurren a disfrazarse para que sea más fácil atraparlos y no sospechen de ellos.

La autora en su tesis “La delincuencia organizada y su prevención. Especial referencia a las pandillas latinoamericanas de tipo violento” declara que una de las causas por la cual no se ha podido frenar el avance del crimen organizado es una defectuosa definición del mismo además de la falta de consenso en la precisión de este crimen en las diferentes legislaciones, así que según el autor lo que los Estados deberían hacer es lograr una definición clara del delito de crimen organizado para que así se puedan establecer medidas que logren la actualización de los medios que tienen los diferentes países para lidiar contra amenazas internacionales tales como el delito de crimen organizado (Córdoba Moreno, 2015).

En mi opinión, las autoridades deberían prestar mas atención a este tipo de actos ilícitos ya que muchas veces se deja pasar por alto o no llega a concluir el proceso por el que tienen que pasar todos los sujetos que lo cometen, es por ello que se requieren de medidas rígidas, aunque ya existan que se respeten tal como está establecido y que se cumplan para así no arrepentirnos luego de la cantidad de crímenes que existen en el país.

En la tesis doctoral “Globalización y transnacionalización de la violencia en Centroamérica: los países del Triángulo Norte” narra que los países con inestabilidad institucional, problema de control de las fronteras, vacíos legales en su normativa y con dificultad de las autoridades y los

diferentes órganos estatales para hacer cumplir la ley son más vulnerables a acciones relacionadas a organizaciones criminales conectadas al narcotráfico, al tráfico de armas y de personas (Mesa Pinedo, 2018).

En mi opinión, la ley se ha ido debilitando de a pocos y no se respeta como se debería, hay cierta cantidad de actos que no llegan a determinarse o no consiguen pruebas necesarias para demostrar que se cometió delitos, cuando las autoridades teniendo el mayor poder deberían concentrarse en reducir este tipo de delitos haciendo respetar la ley y lo que trae consigo.

El autor en su tesis “El papel de la Policía Federal Ministerial en el combate al crimen organizado en Tijuana, durante el periodo 2006-2014” explica que el crimen organizado logra romper la eficacia del estado debido a que estas organizaciones invierten recursos económicos, materiales y humanos para corromper las instancias del gobierno con el fin de obtener resguardo de sus acciones ilícitas lo cual genera una desviación de cualquier actividad política, social y económica de un país. Pone como ejemplo al país de México donde se han observado por los medios de comunicación, diversos casos donde existen vínculos entre los delincuentes con autoridades con el fin de proteger la comisión de este delito el cual genera millones de dólares (Quintana Salazar, 2015).

En mi opinión, la corrupción se encuentra en todos lados y es lamentable ver como las autoridades se dejan comprar e influenciar por personas que le causan daño a muchos ciudadanos, sobre todo al país que ellos deberían sacar adelante, dichas autoridades tendrían que estar implementando nuevas estrategias para combatir este tipo de crímenes, sin embargo, a ellos solo les interesa su dinero y no el bienestar de los ciudadanos.

En la tesis doctoral “La represión penal del crimen organizado: Estrategias metodológicas para judicializar graves violaciones a los derechos humanos” explica que el delito de crimen organizado puede darse de 3 formas: convencional, política e internacional. Informa también que a pesar que el 76% de informes de la Defensoría Pública de Colombia tiene como principales actores las bandas criminales aún no existe un mecanismo político judicial definido en esta materia, señala que no existen estrategias diseñadas unificadas y permanentes de investigación penal que permitan hacer frente a estos casos (Castañeda Díaz, 2016).

La tesis previa pone en evidencia que la policía o institución encargada completamente en la detención de grupos criminales que integran participantes en el país de Colombia, no poseen táctica relevantes y efectivas en su totalidad, por ello se refleja la expansión clara de la delincuencia, que va más allá del sector nacional, pues muchas organizaciones o grupos criminales presentan contactos a nivel internacional que origina el incremento de infracciones y perjudica la situación de seguridad de los países.

La autora en su tesis doctoral en Derecho y Ciencia Política titulada “Investigación y prueba del Ciberdelito” expone que para poder realizar una investigación de delitos informáticos es necesario conocer las cualidades básicas de internet , con lo cual insiste en que se deben realizar capacitaciones para los operadores del derecho y de la justicia; añade además que debido a la naturaleza transnacional de los delitos informáticos es necesario recurrentemente que se creen equipos de investigación aliados o se acudan a instancias internacionales con el fin de investigar y hacer el seguimiento a estos delincuentes (Quevedo González, 2017).

La investigación previa expone que es necesario recurrir a la creación de una institución u organización publica que englobe la formación de profesionales capacitados en el seguimiento de

crímenes realizados virtualmente, específicamente los infractores que se dedican al “cracking” cuya finalidad es perjudicar principalmente en el aspecto financiero y personal a la víctima, para ello se debe reforzar el marco legal de la nación.

Para optar por el título de licenciatura en Derecho con su tesis titulada “Problemática del Delito Informático: Hacia una necesaria regulación internacional.” explican que debido al constante y rápido avance de las tecnologías y los nuevos mecanismos que son utilizados para cometer delitos informáticos, la definición del mismo y como se trata en las diferentes legislaciones es confusa, debido a que existe una falta de comprensión a lo que son realmente estos delitos haciendo que se cataloguen como tal a delitos que no calzan en el tipo penal y por el contrario se deje sin normas a aquellos que si cumplen con los parámetros para ser denominados como tal; por ende recomienda que se debe crear un acuerdo emitido por la ONU con el fin de que se logre regular y unificar una definición de los delitos informáticos y como deben ser tratados por los distintos ordenamientos legales (López Vargas & Milagro, 2010).

En la investigación redactada previamente se manifiesta que los delitos informáticos mantienen un avance veloz al igual que los elementos de la tecnología, las cuales se usan con un fin benéfico, sin embargo, de igual manera que avanza lo positivo, también se desarrolla factores negativos, es por ello que es importante definir concretamente los delitos informáticos y calificarlos analíticamente como el tipo de sanción y delito que se ejecuta.

2.1.2. Nacionales

El autor en su tesis para optar por el título de Magíster en Gobierno y Políticas Públicas titulada “Alternativa para mejorar el proceso de investigación que contribuya a la reducción del accionar del crimen organizado tomando en cuenta la técnica especial de investigación de agente

encubierto” explica que la técnica de investigación del agente encubierto contra organizaciones criminales ha evidenciado resultados positivos cuando se ha utilizado, por ende recomienda que se implementen capacitaciones para la preparación y la formación de agentes encubiertos por parte de la Escuela de Formación Continua de la Policía Nacional del Perú por seis semanas, dos veces al año por tres años seguidos, lo cual permitirá que la PNP tenga personal altamente capacitado y que puedan ser ayudar en la investigación en contra del delito de crimen organizado (López Mendoza, 2018).

En la tesis del autor López Mendoza, se expone una estrategia cuya intención es exponer a los infractores que son partícipes de grupos criminales, la táctica se centra en realizar una técnica policial, donde el colaborador seleccionado será un infiltrado para obtener información de cómo opera dicha banda criminal y visualizar las siguientes operaciones delictivas, que prevalecerán como detalles opcionales ante la detención completa de los infractores, esto refleja ser una estrategia para mejorar la seguridad, sin embargo es necesario que el policía integrado de manera sigilosa y discreta este resguardado por la institución policiaca ante la presencia de irregularidades que pongan en riesgo la vida del colaborador.

En su investigación “Criminalidad Organizada en el Perú: Narcotráfico, Corrupción y otros delitos” concluye que el crimen organizado en sus diversas ramificaciones ha crecido a lo largo de los años teniendo como víctimas principales a las poblaciones más vulnerables y sin que el Estado cree políticas efectivas para frenarlo, esto debido a que las organizaciones criminales han elaborado diversas herramientas para conseguir que las autoridades sean sus cómplices al momento de cometer sus actividades ilícitas, esto último además junto a otros factores como la fragilidad estatal, el proceso ineficiente de la descentralización y el corto alcance en ambientes de difícil acceso hacen que se genere un ambiente idóneo para organizaciones criminales (Torres, 2016).

La investigación previa determina que la mayoría de bandas criminales que continúan realizando actos delictivos sin ser detenidos, son porque presentan conexiones ilegales con las autoridades policiales o incluso con jueces, fiscales y funcionarios públicos, es por ello que realizar una sanción severa a aquellos colaboradores que trabajan en servicio de la función pública y se encuentran participes en situaciones delictivas, por otro lado se necesita visualizar detalladamente y controlar prolongadamente a las instituciones policiales para evitar conflictos internos.

Los autores Loayza y Arapa (2018) en su tesis para optar por el título de Magíster en Gestión Pública titulada “La gestión del conocimiento en la lucha contra el crimen organizado en la región policial Callao. - propuesta de protocolo de investigación del crimen organizado” recomienda que las diferentes regiones policiales adopten un modelo de investigación en base a la teoría de gestión del conocimiento de Nonaka y Takeuchi (1999) así como utilizar técnicas particulares de investigación tales como las medidas de vigilancia y seguimiento, la técnica del agente encubierto, la intervención de comunicaciones, la utilización de softwares y equipos especiales, entre otras, con la finalidad de hacer una lucha efectiva contra las organizaciones criminales.

En la tesis anterior se recomiendan diversos mecanismos que permitan realizar una confrontación eficaz contra las organizaciones criminales además de un modelo de investigación eficiente lo cual debe estudiarse, pero permitiría la desarticulación de muchas organizaciones criminales ya que técnicas como la del agente encubierto o el uso de vigilancia e intervención de comunicaciones han demostrado tener resultados positivos en aquellos casos en que fueron utilizados.

En su tesis para optar por el título de Magister en Derecho Penal titulada “Control de la criminalidad organizada y aplicación en el sistema jurídico penal peruano” recomienda que el

termino de crimen organizado debe ampliarse e incluir otros tipos penales tales como el terrorismo y que al mismo tiempo se debe estudiar la Ley contra el crimen organizado ya que existen muchos vacíos en su aplicación; agrega además que es necesario que se deben crear tanto en el Ministerio Público como en el Poder Judicial órganos especializados cuyo objetivo sea la búsqueda y el seguimiento de organizaciones criminales (Sucari Ccopacondori, 2015).

En la tesis de Sucari, se recomienda que la normativa relacionada con los delitos informáticos sea analizada debido a la existencia de vacíos de derecho cuando se aplica, lo que demuestra la falta de comprensión de manera clara y precisa sobre estos delitos lo cual a su vez puede ocasionar que quienes cometan esta clase de actos ilícitos no sean juzgados o no reciban una pena concordante con sus hechos, por lo cual la recomendación dada en esa investigación acerca del estudio en profundidad de la ley de delitos informáticos me parece importante para poder brindar justicia real a las víctimas de estos delitos.

Los autores en su tesis para optar por el título de Maestro en Informática educativa titulada “Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.” expone que el uso de internet, así como la evolución de la información ha generado ventajas como la globalización y el acceso inmediato a la información pero también genera riesgos relacionados a internet, el desarrollo tecnológico, la gestión de información y la comunicación; uno de estos riesgos son los delitos informáticos los cuales afectan la confiabilidad e integridad de la información y que por ende es necesario se empiecen a elaborar capacitaciones con respecto a seguridad informática (Alarcón Ariza & Antonio, 2017).

La tesis presentada anteriormente además de concluir con que la creación y el avance que ha tenido Internet trae ventajas como desventajas también recomienda que debe enseñárseles a los jóvenes a utilizar de manera segura el internet y las redes sociales desde el colegio, ya que muchas veces son ellos quienes, en su inocencia, son víctimas de estafas o de delitos contra la información, por ende estas recomendación me parece fundamental para un diseño de enseñanza segura respecto del uso de Internet y las redes sociales.

En su tesis para optar por el grado de doctor en Derecho titulada “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” recomienda que el Poder Judicial debe brindar capacitaciones constantes a los operarios del Derecho en contra de los delitos informáticos, específicamente respecto a los principios de protección de la información privada y pública con el objetivo de que estos puedan proteger los derechos fundamentales a aquellos que han visto violados su derecho a la intimidad personal o familiar haciendo uso de la informática (Chávez Rodríguez, 2018).

La investigación descrita previamente concluye con que es fundamental que se capacite de manera continua a los jueces, abogados, y en general aquellos operadores del derecho respecto de las características de los delitos informáticos, esto con el fin de que los aquellos casos donde se hayan cometido estos actos ilícitos puedan resolverse de la mejor manera posible, entendiéndose en su totalidad en qué consisten y cuál es el daño que pueden ocasionar en quien lo sufre.

El autor en su tesis para optar por el título de abogado titulada “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015” explica que el rápido avance de la tecnología ha permitido que los delincuentes informáticos puedan realizar sus actos criminales sin que se les pueda capturar, debido a que se

valen de instrumentos y mecanismos sumamente sofisticados a los cuales aún la legislación del país no se ha adaptado, por ende enfatiza en la necesidad de que el Estado peruano haga parte de convenios y organismos internacionales con los cuales pueda llevar a cabo soluciones eficaces contra este problema, además de darse una capacitación a los miembros de las fuerzas policías para que cuenten con elementos capacitados para detener a estos delincuentes informáticos (Morales Delgado, 2016).

La tesis descrita anteriormente expone la falta de capacidad de adaptación o de avance tecnológico que tiene el país ya que los métodos utilizados por las autoridades competentes para reducir y enfrentar los delitos informáticos son poco sofisticados comparados con los que utilizan los delincuentes para cometerlos, por ende, es necesario que además que se brinden los equipos tecnológicos necesarios para combatir este tipo de delitos, se capacite a las autoridades policiales para que puedan utilizar los mismos de la manera más eficiente posible.

2.2 Bases teóricas

2.2.1. Bases Teóricas sobre Delitos Informáticos

2.2.1.1. *La Teoría del Delito*

En el artículo “Teoría del delito y juicio oral” explica que la teoría del delito es un conjunto de hipótesis que parten de la dogmática para establecer cuáles son los elementos que posibilitan o no el aplicar una consecuencia jurídica a una conducta humana, además explica que el delito se divide en conducta o acción, antijuricidad, culpabilidad y tipicidad, aunque existen diversos autores que agregan a estos la punibilidad; ellos antes explicados son considerados los elementos del delito los cuales no son independientes del delito sino que constituyen su concepto (Calderón Martínez, 2017).

2.2.1.2. *Concepto de delitos informáticos y delitos electrónicos*

En el artículo “Delitos Informáticos” se define a los delitos informáticos y electrónicos como aquellas acciones destinadas a irrumpir los sistemas de seguridad de los dispositivos, tales como la invasión a computadores, correos electrónicos o sistema de datos a través de contraseñas de acceso, las cuales solo pueden llevarse con el uso de la tecnología. En general los delitos informáticos son aquellas conductas en las que la meta, el instrumento o el lugar de ejecución son las TIC (Villavicencio Terreros, 2015).

2.2.1.3. *Las posibles relaciones, la acción dolosa y la acción culposa*

En el artículo “Los delitos culposos” se explica que las acciones dolosas se dan cuando se presume que existe dolo, esto es, la voluntad para cometer un delito con el conocimiento que va en contra de la ley y este se presupone para todos los delitos; sin embargo, existen como excepción las acciones culposas, que se pueden definir como el comportamiento donde no se tiene un cuidado requerido (Ruiz Ramal, 2016).

2.2.1.4. *El delito informático en el código Penal Peruano: art. 186° - A*

En el artículo 186°-A del Código Penal Peruano vigente se tipifica el delito de la decodificación de señales satelitales portadores de programas, en el cual se dará pena privativa de libertad a cualquier sujeto que construya, una, transforme, exporte, importe, venda, distribuya o alquile cualquier sistema cuyo objetivo sea decodificar una señal satelital codificada la cual porte programas siempre y cuando no se tenga la autorización legítima de aquella señal. (Ministerio de Justicia y Derechos Humanos, 2016)

2.2.1.5. Descripción típica y modalidades de los delitos informáticos

En la Ley N° 30171 “Ley de Delitos Informáticos” se precisa que el delito informático se da cuando existen conductas que alteran los sistemas informáticos y otros bienes jurídicos que se cometan con el uso de la tecnología, explica también las diferentes modalidades que existen tales como el delito contra los datos y los sistemas informáticos, contra la libertad sexual y la indemnidad, contra la intimidad y el secretismo de las comunicaciones entre otros (Congreso de la República del Perú, 2014).

2.2.1.6. Delitos informáticos tipificados en el Ordenamiento Jurídico peruano

En la Ley N° 30171 “Ley de Delitos Informáticos” tipifica a los delitos contra datos, sistemas informáticos como la conducta que se da de manera libre para acceder de manera total o parcial o se dañe, introduzca, borre, deteriore, altere o se inutilice de manera parcial o total a un sistema informático siempre que se vulneren las medidas de seguridad establecidas para impedir esta acción ilegal (Congreso de la República del Perú, 2014).

En la Ley N° 30171 “Ley de Delitos Informáticos” se define a los delitos informáticos contra la indemnidad y libertad sexuales como las acciones que se dan a través de cualquier medio análogo a internet para establecer comunicación con un menor de catorce años para pedirle u obtener de él cualquier tipo de material pornográfico o para proponerle cualquier acto sexual (Congreso de la República del Perú, 2014).

En la Ley N° 30171 “Ley de Delitos Informáticos” tipifica la comisión de los delitos informáticos contra la intimidad y el secreto de las comunicaciones cuando se intercepta información de transmisiones privadas, dirigida a un sistema informático, que se originan en un sistema informático o que se realizan dentro del mismo, como también las ondas electromagnéticas

que provengan de un sistema informático que transfiera mencionados datos informáticos (Congreso de la República del Perú, 2014).

En la Ley N° 30171 “Ley de Delitos Informáticos” se define a los delitos informáticos contra el patrimonio cuando se diseña, altera, borra, suprime o se clonan datos informáticos o cuando se da cualquier interrupción o manipulación en el buen funcionamiento de cualquier sistema informático (Congreso de la República del Perú, 2014).

En la Ley N° 30171 “Ley de Delitos Informáticos” se tipifica a los delitos informáticos contra la fe pública como el uso de tecnologías de comunicación o de información para usurpar la identidad de cualquier persona natural o jurídica siempre que se provoque con la misma un perjuicio moral o material (Congreso de la República del Perú, 2014).

En el artículo “El engaño concluyente en el delito de estafa” se explica que el fraude o la estafa es una acción delictiva que se basa en la mentira, información falsa y la confusión continua del proceso que se desea lograr el delincuente hacia la víctima, esta modalidad consta de un plan elaborado cuidadosamente, para evitar una filtración o apariencia de trampa. La mayoría de las situaciones de estafa se centran en el daño económico del perjudicado, que se demuestra en diferentes campos activos, como la inversión en negocios, robo de bienes materiales y extorsiones monetarias (Lux, 2014).

En el artículo “La respuesta penal al ciber fraude, especial atención a la responsabilidad de los muleros del phishing” se expresa el método usado por delincuentes para extraer información privada de un cibernauta a través de mensajes de correo electrónico, recepción de URLs u otros. La información abarca datos confidenciales como tarjetas de crédito, números telefónicos, un seguimiento de transacciones vía internet e incluso datos personales como nombres completos,

edad, dirección y más. Generalmente la mayoría de personas no se percatan al principio pensando que las direcciones de enlace son de confianza, debido a que poseen el nombre de una entidad financiera, pero realmente son delincuentes cibernéticos. Al identificarse los perpetradores, la institución de seguridad cibernética se encarga de la sanción, apegándose al código penal del país de España, como otro punto relevante, esta modalidad es muy común en la mayoría de países (Llinares, 2013).

2.2.2. Bases teóricas de Crimen Organizado:

2.2.2.1. *Concepto*

En “Política Nacional Multisectorial de lucha contra el Crimen Organizado 2019 - 2030” se define al crimen organizado como las actividades ilícitas cometidas por una agrupación de tres o más personas que se reparten diversas tareas, añade que el crimen organizado controla cierto territorio y se inserta en los mercados formales e informales para insertar sus ganancias y burlar los controles del Estado (Ministerio del Interior del Perú, 2019).

2.2.2.2. *Naturaleza jurídica del crimen organizado*

En el artículo “El crimen organizado: un concepto extraño al derecho penal argentino” se explica que no se tiene definida cual es la naturaleza del delito de crimen organizado ya que una gran variedad de personas, eventos y estructuras están subsumidos dentro de este concepto, por ende el crimen organizado se dirime de la realidad social a la que debería estar ceñido, lo que hace que los estudiosos de la materia no solo deben definir un único concepto sino que además deben luchar contra la dualidad de la expresión crimen organizado como algo concerniente a la realidad social o como una construcción social (Cordini, 2017).

2.2.2.3. Características del crimen organizado

2.2.2.3.1. Líneas distintivas de la criminalidad organizada y diferencias con la banda criminal

En el artículo “¿Cuáles son las diferencias entre banda criminal y organización criminal?” se explica la diferencia entre una banda criminal y una organización criminal, la semejanza entre ambas es que poseen una estructura criminal sin embargo la primera es una de menor complejidad organizativa, la cual realiza un plan para delinquir menos trascendente y propio de la delincuencia urbana común, por lo cual se diferencia de la segunda debido a que no pretende mantener negocios ilegales sino que producen inseguridad a través de actos de violencia y despojo artesanal, por ende posee una cantidad de miembros reducido y basado en la violencia. (Tumi Pacori, 2020)

2.2.2.3.2. Características propias de la criminalidad organizada

En el artículo “Conceptualización del Crimen Organizado y su regulación en la legislación Penal Colombiana” se explican que las características propias del crimen organizado son las siguientes: debe existir una pluralidad de agentes para la comisión del delito pero no puede considerarse a cualquier pluralidad sino a aquellas que están firmemente estructuradas; esta pluralidad llamada también organización debe tener un objetivo criminal común; debe tener una duración definida en el tiempo y por último debe existir una finalidad lucrativa, esto es el propósito final de la organización criminal y de sus miembros debe ser lucrar de manera ilícita (Scheller D'angelo & Lugo Quiroz, 2019).

En el artículo “Los criterios para la mensuración del valor del enriquecimiento ilícito y perjuicios causados por actos corruptos” manifiesta que los actos de corrupción son comunes en

organizaciones que generan ingresos altos, ya sea de característica pública o privada la institución, la respuesta del sistema judicial debe ser inmediata, llevando a cabo un proceso de investigación con los responsables de la discutible acción presentada, teniendo como resultado concluyente una sanción severa (Mendonça, 2016).

2.2.2.4. Objetivos de las organizaciones criminales

En el artículo “Crimen organizado: una aproximación al fenómeno” se expone que el objetivo de las organizaciones criminales es perdurar en el tiempo para continuar con la comisión de delitos para obtener beneficios, por ende, la organización solo se justifica en la medida que sea rentable para sus miembros, por ende, se actúa racionalmente y con cierto grado de complejidad y de planificación, por ende, detrás de cada movimiento existe premeditación y planeación (Jiménez Serrano, 2015).

2.2.2.5. Formas de organización criminal

En el artículo “¿En qué consiste una organización criminal y cómo opera la imputación de responsabilidad a sus miembros?” se explica que existen varios tipos de organizaciones criminales, tanto con estructuras horizontales, las cuales se caracterizan por ser flexibles y tener una gran distribución del poder e información entre sus integrantes; y las de estructuras verticales que son severas respecto a la división de tareas; actualmente las primeras van imponiéndose sobre las segundas. (Hurtado Paico, 2018)

2.2.2.5.1. Etapa Predatoria

En el artículo “El Crimen Organizado Transnacional (COT) en América del Sur. Respuestas regionales” explica que esta es la primera etapa del crimen organizado donde la organización

criminal toma el control de un territorio para defender la ilegalidad de sus acciones, elimina a su vez a los que consideran posibles amenazas o competidores, consiguen influencia en la sociedad y la política y se garantizan su supervivencia (Riquelme Rivera, Salinas Cañas, & Franco Severino, 2018).

En el artículo “La Argentina y las etapas del narcotráfico” se explica que esta fase se distingue debido a que la organización se afianza en un territorio y esto garantiza su poder a través del uso de violencia con lo cual logra ganar influencia de la localidad donde se encuentra, defiende la empresa ilícita, elimina contrincantes y elabora un monopolio del uso privado de la fuerza. Además, posee una estructura estructuralmente empobrecida y el poder es ejercido por los miembros más antiguos. (Tokatlian, 2015)

2.2.2.5.2. *Etapas Parasitaria*

En el artículo “El Crimen Organizado Transnacional (COT) en América del Sur. Respuestas regionales” explica que, en la segunda fase, la parasitaria, se incrementa de manera importante la influencia dentro de la política y la economía corrompiendo a diversas instituciones tanto del sector público como del privado con el fin de obtener su legitimación, democratización y su extensión (Riquelme Rivera, Salinas Cañas, & Franco Severino, 2018).

En el artículo “La Argentina y las etapas del narcotráfico” se explica que al no detectar y detener a tiempo a la organización en la primera etapa, esta llega a avanzar hacia la segunda donde buscan su legitimación, esto es, la aceptación y el reconocimiento por parte de la sociedad donde se encuentran; la proliferación con la diversificación de las inversiones en empresas legales; y por último la democratización, esto es la reproducción de diversas organizaciones, desde grandes carteles hasta pequeñas organizaciones con diversos tipos de jerarquía (Tokatlian, 2015).

2.2.2.5.3. *Etapa simbiótica*

En el artículo se explica que por último se tiene la fase simbiótica donde la organización criminal se afianza definitivamente en el sistema político y económico con lo cual se apodera del Estado y este último se pone al servicio de los delincuentes, en resumen, el Estado y la organización criminal son casi lo mismo (Riquelme Rivera, Salinas Cañas, & Franco Severino, 2018).

En el artículo se expone que si el país donde se encuentra la organización criminal no cuenta con la suficiente voluntad, recursos o la capacidad para detenerla, es sumamente probable que se llegue a la tercera fase donde el sistema económico y político se vuelven tan dependientes del crimen organizado, entonces el Estado de derecho se estabiliza y el crimen organizado a pesar de no atrapar plenamente a un Estado si lo logra con muchas provincias o regiones del mismo y se crea una nueva clase social que desestabiliza el orden estatal (Tokatlian, 2015).

2.2.2.6. *El crimen organizado transnacional*

En el artículo “El Crimen Organizado Transnacional (COT) en América del Sur. Respuestas regionales” se determina que los delitos o la cualidad de transaccionalidad del crimen organizado es muy amplio ya que pueden referirse por ejemplo a delitos que se cometen en más de un país como a aquellos que se cometen en un Estado pero que quien o quienes los cometen operan en más de un Estado y a su vez son aquellos delitos que se dan en un Estado o país pero que genera consecuencias sustanciales en otro país o Estado (Riquelme Rivera, Salinas Cañas, & Franco Severino, 2018).

2.3 Definición de Términos Básicos

2.3.1. Delitos Informáticos

El delito informático no solo se refiere a la comisión de una conducta delictiva con el uso de instrumentos o medios informáticos o a los procederes ilícitos en los que ellos sean su objeto; sino que se refiere también al perjuicio de la información (Suárez Sánchez, 2009).



Figura 1: Delitos Informáticos

Los ciberdelincuentes o también conocidos como hackers utilizan la vulnerabilidad de cualquier página o servidor web para suprimir, introducir, alterar, apropiar, deteriorar o hacer inaccesible cualquier tipo de dato informático o de información, con el fin de obtener un beneficio para sí mismo o para un tercero (Portilla Marzano & Taboada Cárdenas, 2020).

2.3.1.1. Conductas Maliciosas

Las conductas maliciosas son aquellas conductas antisociales que perjudican el derecho de otras personas o que ponen en peligro el bienestar del individuo que las comete o de la comunidad,

con estas conductas se tiende a violar las leyes a las que está sujeto el individuo (Valgañón, Muños, & Briccola, 2014).

Figura 2: Conductas Maliciosas

Las conductas maliciosas suelen ser cometidas en su mayoría por hombres, además que



existe una alta tendencia de comisión de estas conductas por jóvenes de entre 14 a 17 años, los cuales acuden a estas organizaciones criminales con el fin de obtener beneficios económicos de manera rápida. (Sánchez Velasco, Galicia Moyeda, & Robles Ojeda, 2017).

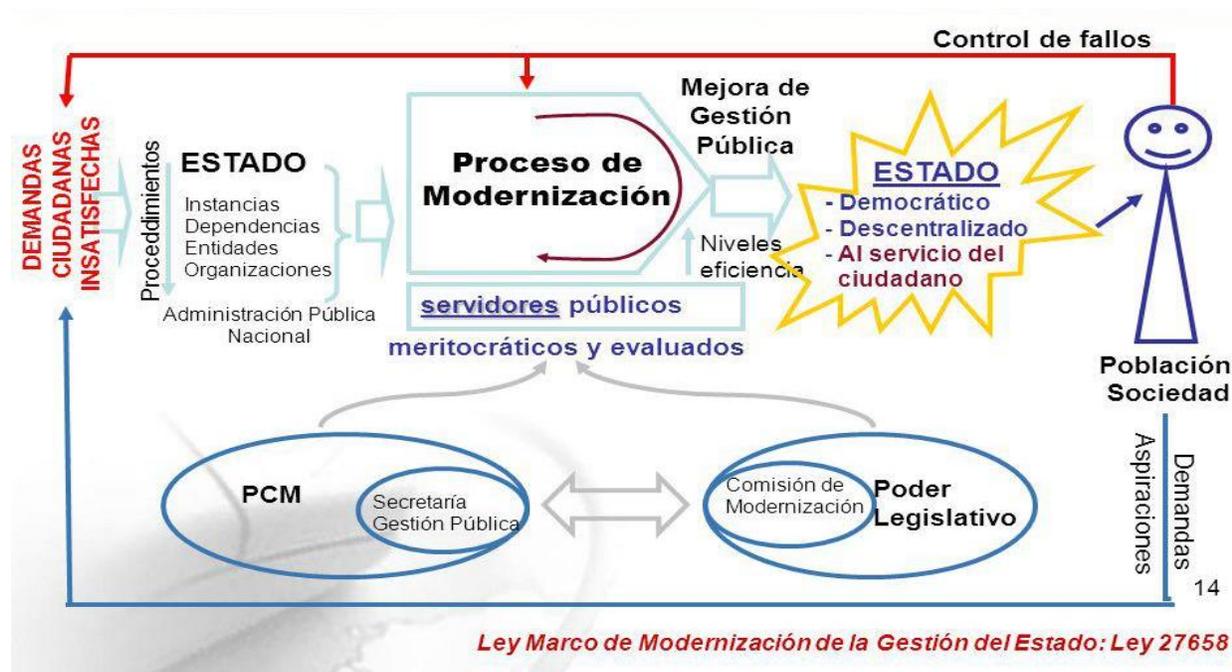
2.3.1.1.1. Necesidad de modernizar leyes

En el libro “XXIII Jornadas de estudio. La modernización de la justicia en España. XXIV Jornadas de estudio. El ámbito privado del sector público” se explica que las leyes regulan las relaciones que se dan en la sociedad, por ende, respecto a que las relaciones dentro de la sociedad

son variantes a lo largo del tiempo es necesario que las leyes también posean una tendencia de cambio con el fin de salvaguardar el respeto a la dignidad de las personas y el Estado de derecho (Ministerio de Justicia de España).

Figura 3: Necesidad de modificar leyes

En la figura se puede observar cual es el plan que tiene el Estado peruano para lograr una modernización de su gestión, todo esto estipulado en la Ley N°27658 – Ley de Modernización de



la Gestión del Estado (Quillama Torres, 2008).

2.3.1.1.2. Explotación de datos personales

Según el libro “Seguridad informática y protección de datos personales” la explotación de datos personales se da cuando algunas personas se introducen de manera ilegal a los sistemas con el fin de robar datos confidenciales que se almacenan en ellos para usarlos a su beneficio; es por

esto que se deben conocer y aplicar las medidas necesarias para asegurar que nuestros sistemas informáticos cuenten con la mayor seguridad posible (Iñiguez Estrada, 2020).

Figura 4: Explotación de datos personales

Lo que se aprecia en la figura es lo que se denomina actualmente como Black Hat (Hacker de sombrero negro) los cuales se dedican a robar información confidencial que se almacenan en



los sistemas informáticos con el fin de usarlo para su beneficio o el de un tercero (Lampstudy, 2020).

2.3.1.2. Crimen Electrónico

El crimen electrónico es aquella acción antijurídica imputable y culpable que se realiza mediante el uso de vías informáticas y diversos recursos cibernéticos y electrónicos que tienen

como meta el dañar medios informáticos, computadores, y redes de internet para extraer, modificar o dañar información de las víctimas (Chauca Acero, 2014).

Figura 3: Crimen Electrónico

Almacenar archivos en la nube, tener cuidado con los correos electrónicos que se reciben,



la dificultad en las contraseñas, mantener los dispositivos electrónicos actualizados y estar alerta respecto a las páginas web donde se realicen compras por Internet son recomendaciones que se deben tener en cuenta para no ser víctima de un crimen electrónico (Arenas, 2020).

2.3.1.2.1. Estafa

En el libro “Grandes maestros de la estafa” se define a la estafa como la conducta delictiva en la cual se da una defraudación causada por medio de un engaño o ardid; precisando el engaño en diferentes formas tales como el nombre supuesto, la calidad simulada, los títulos falsos la

influencia mentida, el abuso de confianza o el aparentar bienes, créditos, comisiones, empresas o negociación o utilizando cualquier otro engaño o ardid (Durigon, 2016).

Figura 6: Estafa

En la imagen se puede observar lo que se conoce como la estafa del CEO, la cual se basa en engañar a un cargo alto de alguna empresa con un correo electrónico donde se simula ser su jefe



o CEO, en el correo se solicita se haga una transacción secreta y urgente a un número de cuenta, el cual pertenece a los estafadores (Garcia, 2020).

2.3.1.2.2. Beneficio ilícito

En el libro “Propuestas penales: nuevos retos y modernas tecnologías” se expone que el delito del beneficio o enriquecimiento ilícito consiste en el incremento del patrimonio el cual no puede ser razonable ni legalmente justificado, explica también que algunos autores sostienen que

el bien jurídico que se vulnera la imagen de transparencia, gratuidad y probidad (Pérez Álvarez, Díaz Cortés, Heredero Campo, & Villasante Arroyo, 2016).

Figura 7: Beneficio ilícito

El beneficio económico de manera ilícita es el fin de las personas u organizaciones que realizan los crímenes informáticos debido que con los resultados de las mismas sea viable seguir cometiendo



más delitos con el pasar del tiempo, en cuanto la comisión del delito no sea beneficiosa esta pierde su sentido (Novoa, 2015).

2.3.2. Crimen Organizado

El crimen organizado se conforma por tres o más personas que poseen los mecanismos y la organización para actuar de manera ilegal dentro de las actividades políticas y económicas, cuya influencia se extiende hasta tal punto que condicionan de manera negativa a sectores amplios de la sociedad en niveles productivos e institucionales (Martínez Martínez, 2015).



Figura 4: Crimen Organizado

En la imagen podemos observar a todos los integrantes acusados de pertenecer a la organización criminal de “Los Cuellos Blancos del Puerto” conformados por diversos abogados, servidores públicos y empresarios; la cual se habría formado para brindar sentencias favorables o designaciones a cargos específicos a cambio de ganancias económicas (Bazo Reisman, 2018).

2.3.2.1. Jerarquía estructurada

Dentro de las organizaciones criminales existen diversas formas de jerarquía, específicamente cinco; la primera, la jerarquía estándar donde existe un líder y todos los miembros poseen roles claramente definidos; la jerarquía regional, donde además del líder principal existen líderes por regiones; la agrupación jerárquica, donde existen varios grupos criminales y las

decisiones se toman en conjunto por un representante de cada grupo; el grupo central donde no existe un líder y las decisiones se toman por acuerdo; y por un último la red criminal (Hurtado Paico, ¿En qué consiste una organización criminal y cómo opera la imputación de responsabilidad a sus miembros?, 2018).

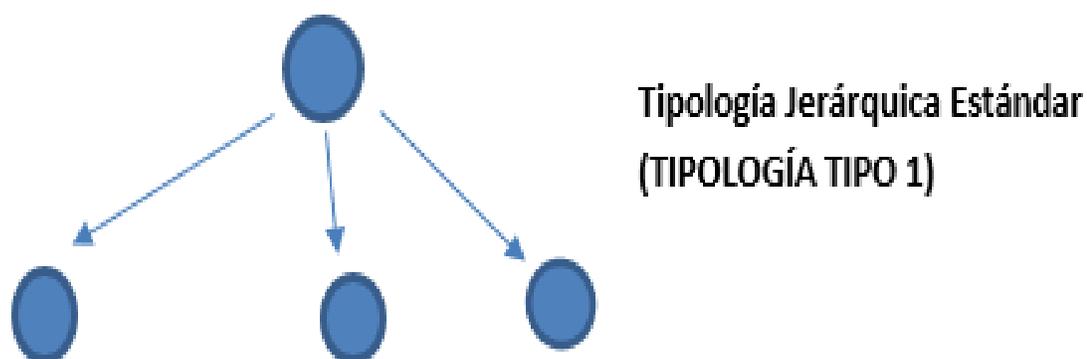


Figura 5: Jerarquía Estructurada

En la imagen podemos observar el tipo de jerarquía más usada dentro de las organizaciones criminales, la cual es la jerarquía estándar o de tipología 1 donde la organización es vertical rígido con la existencia de un líder y roles claramente definidos para cada uno de los miembros (Hurtado Paico, 2018).

2.3.2.1.1. Intervención delictiva

En el libro “Autores, partícipes y superiores en la Justicia Transicional” se explica que dentro de los grupos denominados como organizaciones criminales existen diversos grados de intervención delictiva, así tenemos a los autores o coautores, a los cómplices primarios y los cómplices secundarios, los cuales poseen determinadas funciones dentro de la organización (Marxen, 2018).

Autoría, autoría mediata y coautoría

- **Artículo 23.-** *El que realiza por sí o por medio de otro el hecho punible y los que lo cometan conjuntamente serán reprimidos con la pena establecida para esta infracción.*

Instigación

- **Artículo 24.-** *El que, dolosamente, determina a otro a cometer el hecho punible será reprimido con la pena que corresponde al autor.*

Complicidad primaria y complicidad secundaria

- **Artículo 25.-** *El que, dolosamente, preste auxilio para la realización del hecho punible, sin el cual no se hubiere perpetrado, será reprimido con la pena prevista para el autor.*
- *A los que, de cualquier otro modo, hubieran dolosamente prestado asistencia se les disminuirá prudencialmente la pena.*

Figura 10: Intervención Delictiva

En la figura se puede observar como el Código Penal Peruano vigente regula los diferentes grados de participación de la intervención delictiva, tanto de la autoría, la instigación y la complicidad primaria y secundaria (Ministerio de Justicia y Derechos Humanos, 2016).

2.3.2.1.2. Planificación

En el libro “El delito de organización terrorista: Un modelo de Derecho penal del enemigo” se explica que las organizaciones criminales requieren de planificación previa que a su vez requieren de estabilidad para su creación, esto además con el objetivo de que dentro de la organización criminal exista el concierto y la coordinación lo cual les permitirá realizar sus acciones criminales con una mayor efectividad (Santa Rita Tamés, 2015).

ORGANIGRAMA DEL SECTOR DE OPERACIONES ESTRUCTURADAS

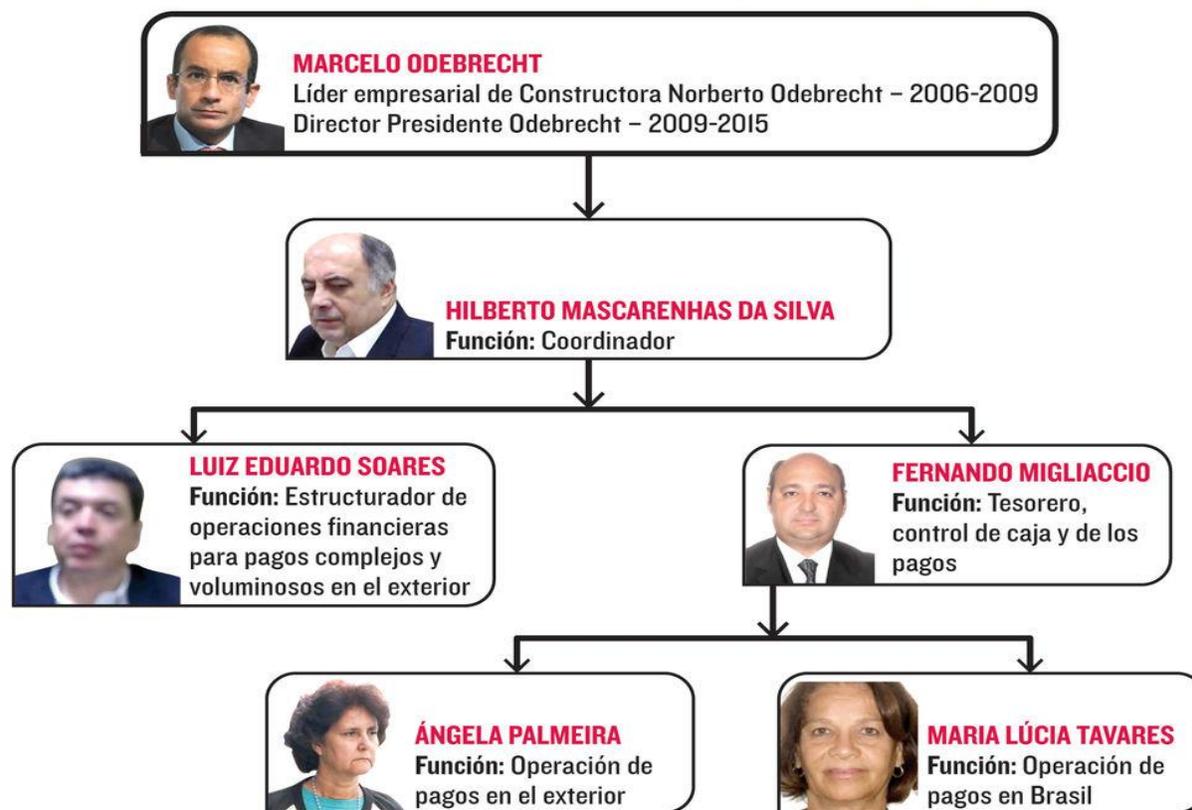


Figura 11: Planificación

En la imagen podemos observar el grado de planificación que tenía la organización criminal de la empresa constructora Odebrecht la cual tuvo implicancias también en nuestro país, como se puede observar existe una clara repartición de tareas además de una verticalizada estructura, signos de una planificación (Gorriti, 2019).

2.3.2.2. Transnacionalidad

La transnacionalidad de un delito es un término amplio, pero puede referirse a la comisión de un delito en más de un país, como también a la comisión del delito en un país pero que es llevado a cabo por una organización que opera en más de un Estado, o a los actos delictivos que se cometen en un país pero que afectan de manera grave a otro país (UNODC, 2020).

En 2016

- Principales países de procedencia según las incautaciones
- ➔ El tamaño de las líneas corresponde a la cantidad incautada de cocaína y el número de menciones de países de donde partió.

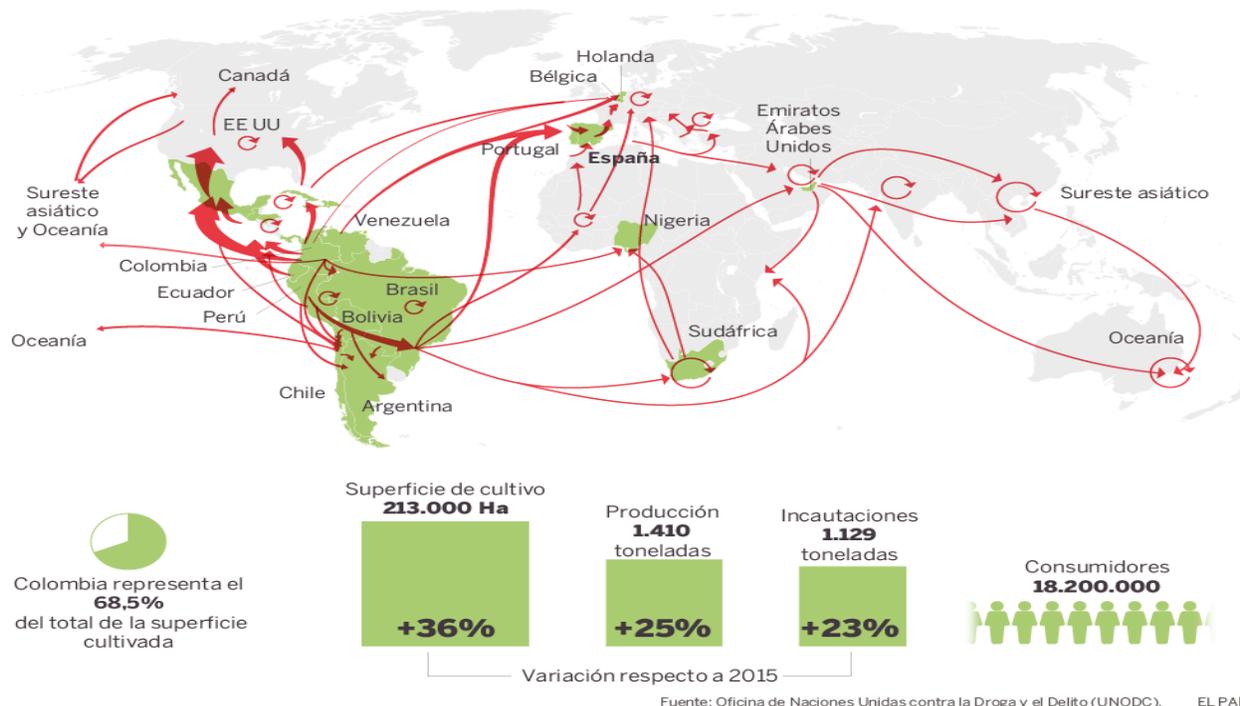


Figura 6: Transnacionalidad

Las organizaciones criminales con más alcance a nivel internacional son las relacionadas con el tráfico de drogas, en la imagen podemos ver cómo es que la cocaína circuló alrededor del mundo en el año 2016 precisamente gracias a este componente de la criminalidad organizada (Diario El País, 2018).

2.3.2.2.1. Extorsiones Delictivas

En el libro “Derecho penal aplicado. Parte especial. Delitos contra el patrimonio y contra el orden socioeconómico” se explica que la extorsión es el delito en el cual con ánimo de lucro se use la violencia o la intimidación con el fin de obligar a otro a realizar u omitir un acto en perjuicio de su patrimonio o el de un tercero (Perrino Perez, Fernandez Agudo, & Jaen Vallejo, 2018).



Figura 13: Extorsiones delictivas

Las extorsiones con amenaza a través de los teléfonos celulares son la modalidad más común de este delito, muchas veces los extorsionadores son personas encarceladas que logran conseguir los aparatos tecnológicos para lograr su cometido; cuando se es víctima de una extorsión debe hacerse la denuncia inmediatamente ya que de lo contrario no se iniciarán las investigaciones para identificar el emisor de las amenazas (RPP Noticias, 2020).

2.3.2.2.2. Grupos criminales

En el libro “Criminalidad organizada y terrorismo. Formas criminales paradigmáticas” se explica que los grupos criminales son agrupaciones de dos o más personas que poseen por objetivo y finalidad la comisión de delitos y que operan con una falsa apariencia de conformidad con la ley aumentando de manera cuantitativa y cualitativa la lesividad y el daño de sus conductas (López Muñoz, 2019).



Figura 14: Grupos criminales

En la imagen se pueden observar los grupos criminales más peligrosos de Latinoamérica, encabezado por el Ejército de Liberación Nacional, el cual ocupa el primer puesto debido a que ha logrado expandirse por todo Colombia y Venezuela (McDermott, 2020).

Capítulo III: Marco Metodológico

3.1 Enfoque de la Investigación

El trabajo de investigación actual se ha realizado bajo el enfoque cuantitativo. Este enfoque recolecta datos para validar la hipótesis basándose en la medición numérica y el análisis de estadísticas, esto con el objetivo de fijar patrones de comportamiento y probar teorías. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014).

Se aplicará la técnica de la encuesta de opinión para lo cual se usará un cuestionario que contiene 16 preguntas para la recolección de datos, esto con el fin de entablar una relación entre los delitos informáticos y el crimen organizado en el distrito de San Isidro 2020.

3.2 Variables

3.2.1. Operacionalización de variables.

3.2.1.1. Variable independiente (X-1).

- Delitos Informáticos

3.2.1.1.1. Dimensiones

- Conductas maliciosas.
- Crimen electrónico.

3.2.1.1.2. Indicadores.

- Necesidad de modernizar leyes
- Explotación de datos personales
- Estafa

- Beneficio ilícito

3.2.1.2. Variable dependiente (Y-2).

Crimen Organizado

3.2.1.2.1. Dimensiones

- Jerarquía Estructurada
- Transnacionalidad

3.2.1.2.2. Indicadores.

- Intervención delictiva
- La planificación
- Extorsiones delictivas
- Grupos criminales

Tabla 1

Operacionalización de las variables

Variable	Definición conceptual	Definición operacional	Dimensión	Indicador	Ítem	Instrumento	Escala	Niveles de rango
Delitos Informáticos	El delito informático no solo se refiere a la comisión de una conducta delictiva con el uso de instrumentos o medios informáticos o a los procedimientos ilícitos en los que ellos sean su objeto; sino que se refiere también al perjuicio de la información de la información (Suárez Sánchez, 2009).	Los delitos informáticos comprenden dos dimensiones respecto a conductas maliciosas y el crimen electrónico.	Conductas maliciosas	Necesidad de modernizar leyes	1, 2	Cuestionario	(1) Totalmente de acuerdo (2) de acuerdo (3) no de acuerdo, ni en desacuerdo (4) en desacuerdo (5) Totalmente desacuerdo	Mala 8 - 18 Regular 19 - 29 Buena 30 - 40
				Explotación de datos personales	3, 4	Cuestionario		
			Crimen electrónico	Estafa	5, 6	Cuestionario		

			Beneficio ilícito	7, 8	Cuestionario			
Crimen Organizado	Se conforma por tres o más personas que poseen los mecanismos y la organización para actuar de manera ilegal dentro de las actividades políticas y económicas, cuya influencia se extiende hasta tal punto que condicionan de manera negativa a sectores amplios de la sociedad en niveles productivos e institucionales (Martínez Martínez, 2015).	El crimen organizado comprende dos dimensiones que corresponden a la jerarquía estructurada y la transnacionalidad.	Jerarquía Estructurada	Intervención delictiva	9, 10	Cuestionario	(1) Totalmente de acuerdo	
				La planificación	11, 12	Cuestionario	(2) de acuerdo	Mala 8 - 18
				Extorsiones	13, 14	Cuestionario	(3) no de acuerdo, ni en desacuerdo	Regular 19 - 29
			Transnacionalidad	Grupos criminales	15,16	Cuestionario	(4) en desacuerdo	Buena 30 - 40
								(5) Totalmente desacuerdo

Fuente: Elaboración propia

3.3 Hipótesis

1.3.1. Hipótesis General.

- La influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro - 2020.

1.3.2. Hipótesis Específicas.

- La necesidad de modernizar leyes influye en la intervención delictiva del crimen organizado en el distrito de San Isidro- 2020
- La explotación de datos personales influye en la planificación de las organizaciones criminales en el distrito de San Isidro - 2020.
- La estafa influye en las extorsiones delictivas en las extorsiones delictivas transnacionales del crimen organizado en el distrito de San Isidro- 2020.
- El beneficio ilícito influye en los grupos criminales transnacionales del crimen organizado en el distrito de San Isidro- 2020.

3.4 Tipo de Investigación

El tipo de investigación del presente proyecto es aplicada no experimental de enfoque cuantitativo, ya que se analizan e indaga las variables planteadas en su propio contexto sin manipularlas (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014).

3.5 Diseño de la investigación

El presente trabajo de investigación tuvo un diseño no experimental transaccional correlacional, ya que se busca explicar la relación entre las variables delitos informáticos y crimen organizado (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014).

3.6 Población y Muestra

3.6.1. Población.

La población estuvo conformada por 50 personas que laboran y concurren continuamente a la comisaría de San Isidro ubicada en Calle Antequera 116, San Isidro.

3.6.1.1. Criterios de inclusión.

Personas que laboran o concurren a la comisaría de San Isidro, asimismo se centró en participantes como autoridades policiales.

3.6.1.2. Criterios de exclusión.

Personas que no pertenecen, laboran u otros ciudadanos que no hayan concurrido a la comisaría de San Isidro.

3.6.2. Muestra.

En la presente investigación se consideró al total de la población descrita anteriormente, por lo que no hubo muestra.

3.7 Técnicas e Instrumentos de Recolección de Datos

Para la presente investigación se aplicó la técnica de la encuesta de opinión mediante aplicativos que constan de la necesidad de internet, correos electrónicos para una formalidad ejemplar, asimismo está construida a base de 16 preguntas cerradas con alternativas de respuesta son de tipo Likert (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014).

3.7.1. Técnica.

Se estableció para esta investigación la técnica de encuesta de opinión mediante un cuestionario el cual contiene 16 preguntas cerradas con respuesta de tipo Likert. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014)

3.7.2. Instrumento de recolección de datos.

3.7.2.1. Análisis de fiabilidad del instrumento

Tabla 2

Estadísticos de fiabilidad del instrumento

Alfa de Cronbach	N de elementos
,970	16

Posteriormente de aplicar el análisis de fiabilidad al instrumento usado en este proyecto de investigación tenemos como resultado 0.970 como se visualiza en la Tabla 2, y este valor es

considerado muy alto por lo que podemos afirmar que el instrumento aplicado que cuenta con 16 preguntas es fiable.

3.7.2.2. Validez del instrumento

Tabla 3

El instrumento aplicado en la presente investigación fue validado mediante

Validación del instrumento de recolección de datos por juicio de expertos

Experto	Apellidos y nombres	Grado académico	Resultado
1	Morales Gallo, Martín	Maestro	Aplicable
2	Santamaría Portocarrero, Walter	Maestro	Aplicable

Fuente: elaboración propia

Capítulo IV: Resultados

4.1 Análisis de los Resultados

4.1.1. Distribución de frecuencia.

Tabla 4

Pregunta 01: ¿Considera usted que es necesario modernizar las leyes debido a que con el paso del tiempo aparecen nuevos delitos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	32	64,0	64,0	64,0
	De acuerdo	18	36,0	36,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

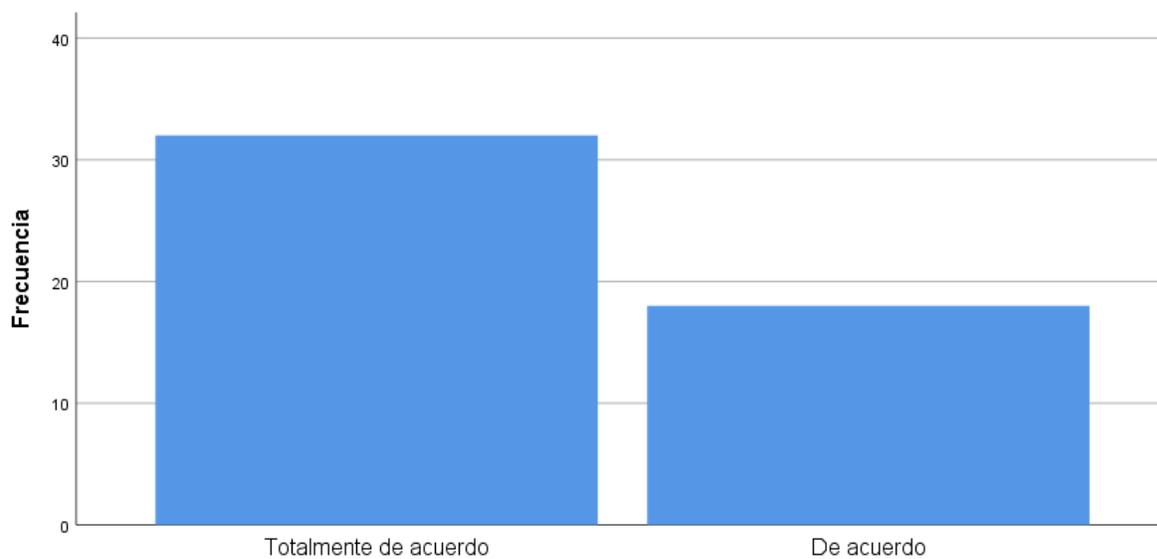


Figura 7: Gráfico de barras de la Pregunta 01. ¿Considera usted que es necesario modernizar las leyes debido a que con el paso del tiempo aparecen nuevos delitos? Fuente: Elaboración propia – SPSS

De 50 encuestados se visualiza que 32 de ellos estuvieron totalmente de acuerdo que es necesario modernizar las leyes debido a que con el paso del tiempo aparecen nuevos delitos. Como se aprecia en la tabla 4 y figura 7

Tabla 5

Pregunta 02: ¿Está usted de acuerdo en que se deben incorporar más leyes para regular los delitos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	33	66,0	66,0	66,0
	De acuerdo	17	34,0	34,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

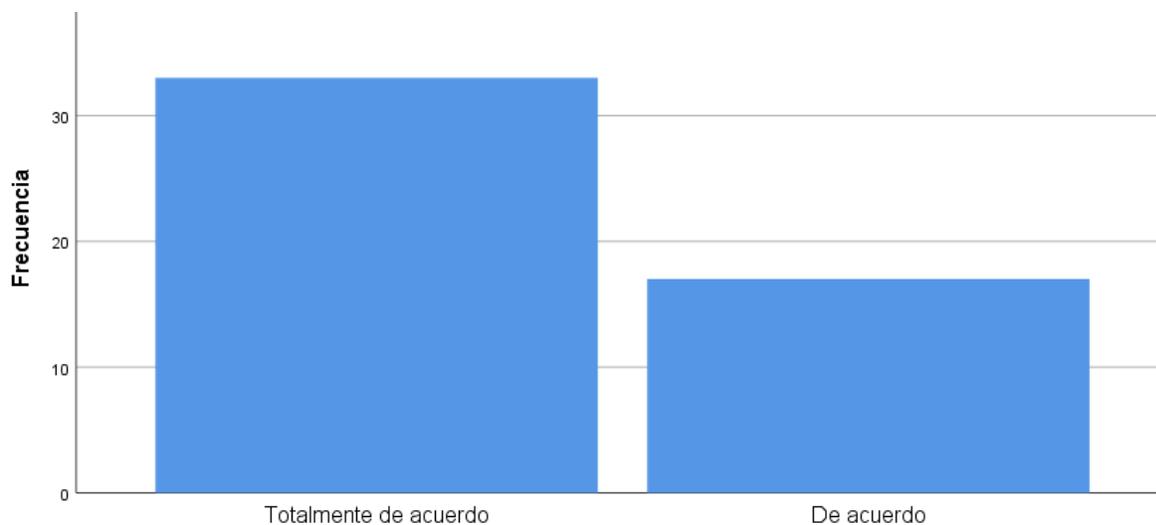


Figura 8: Gráfico de barras de la Pregunta 02: ¿Está usted de acuerdo en que se deben incorporar más leyes para regular los delitos informáticos? Fuente: Elaboración propia – SPSS

Del 100 % de encuestados, se evidencia que un 66,0 % estuvieron totalmente de acuerdo que se deben incorporar más leyes para regular los delitos informáticos. Asimismo, se puede observar los resultados en la tabla 5 y figura 8.

Tabla 6

Pregunta 03: ¿Cree usted que el mal uso de la explotación de datos personales constituye una grave falta a la integridad de la persona?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	37	74,0	74,0	74,0
	De acuerdo	13	26,0	26,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

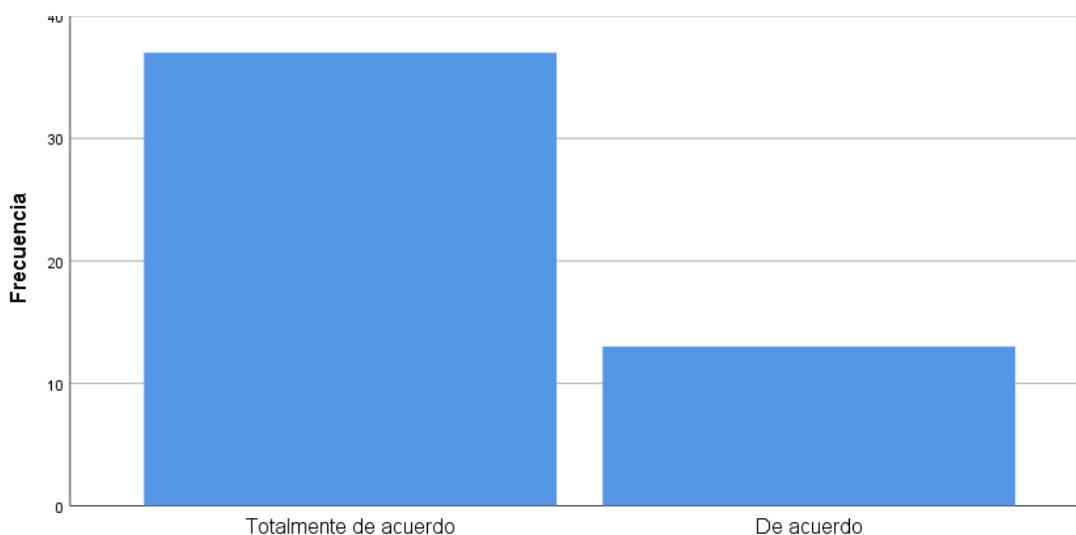


Figura 9: Gráfico de barras de la Pregunta 03: ¿Cree usted que el mal uso de la explotación de datos personales constituye una grave falta a la integridad de la persona? Fuente: Elaboración propia – SPSS

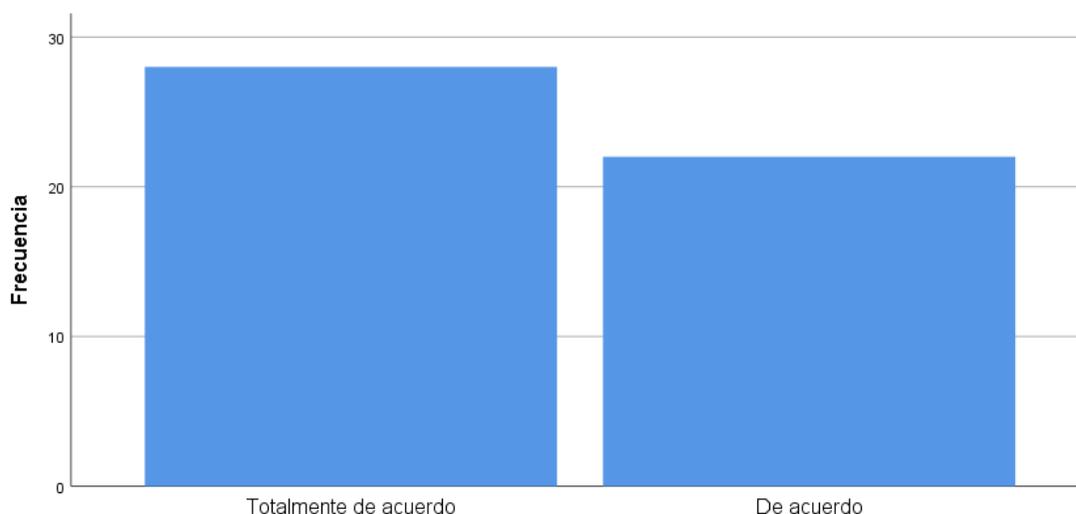
De 50 encuestados, 37 colaboradores coincidieron que el mal uso de la explotación de datos personales constituye una grave falta a la integridad de la persona. Para la visualización de los datos se puede observar la tabla 6 y figura 9.

Tabla 7

Pregunta 04: ¿Piensa usted que la explotación de datos personales ocurre porque muchas personas no tienen el conocimiento sobre medidas de seguridad en los sistemas informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	28	56,0	56,0	56,0
	De acuerdo	22	44,0	44,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS



*Figura 10: Gráfico de barras de la Pregunta 04: ¿Piensa usted que la explotación de datos personales ocurre porque muchas personas no tienen el conocimiento sobre medidas de seguridad en los sistemas informáticos?
Fuente: Elaboración propia – SPSS*

Del 100 % de encuestados, un 56 % estuvo totalmente de acuerdo que la explotación de datos personales ocurre porque muchas personas no tienen el conocimiento de acuerdo sobre los sobre medidas de seguridad en los sistemas informáticos. Se puede visualizar los datos en la tabla 7 y figura 10.

Tabla 8

Pregunta 05: ¿Considera usted que el principal objetivo de los delitos informáticos es la estafa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	27	54,0	54,0	54,0
	De acuerdo	23	46,0	46,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

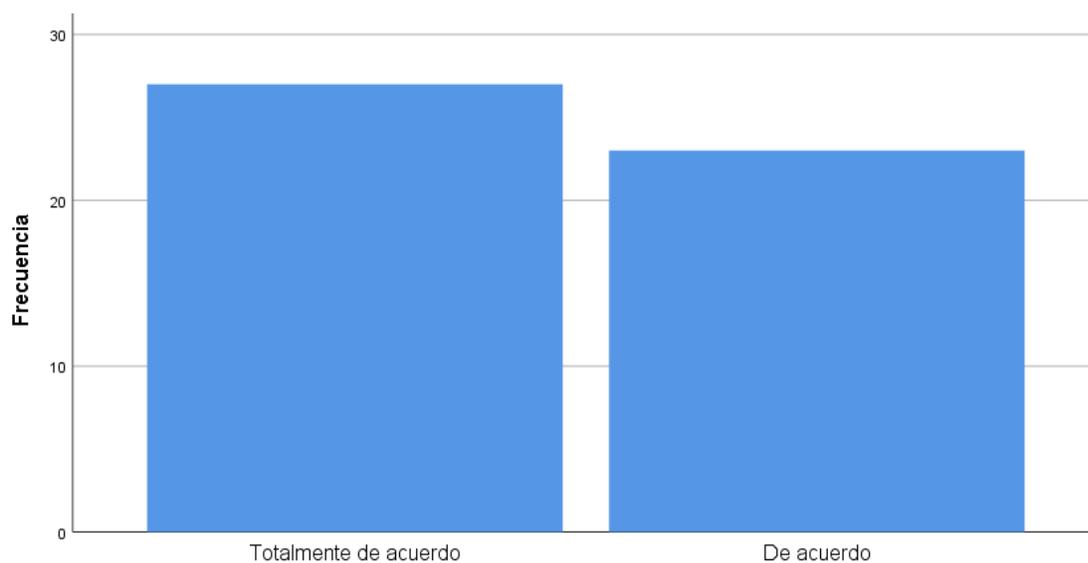


Figura 11: Gráfico de barras de la Pregunta 05: ¿Considera usted que el principal objetivo de los delitos informáticos es la estafa? Fuente: Elaboración propia – SPSS

De 50 encuestados, 27 participantes del cuestionario estuvieron totalmente de acuerdo que principal objetivo de los delitos informáticos es la estafa. Asimismo, se visualizan los datos en la tabla 8 y figura 11.

Tabla 9

Pregunta 06: ¿Está usted de acuerdo en que las principales víctimas de estafa son los adultos mayores?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	33	66,0	66,0	66,0
	De acuerdo	12	24,0	24,0	90,0

Ni de acuerdo ni en desacuerdo	4	8,0	8,0	98,0
En desacuerdo	1	2,0	2,0	100,0
Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

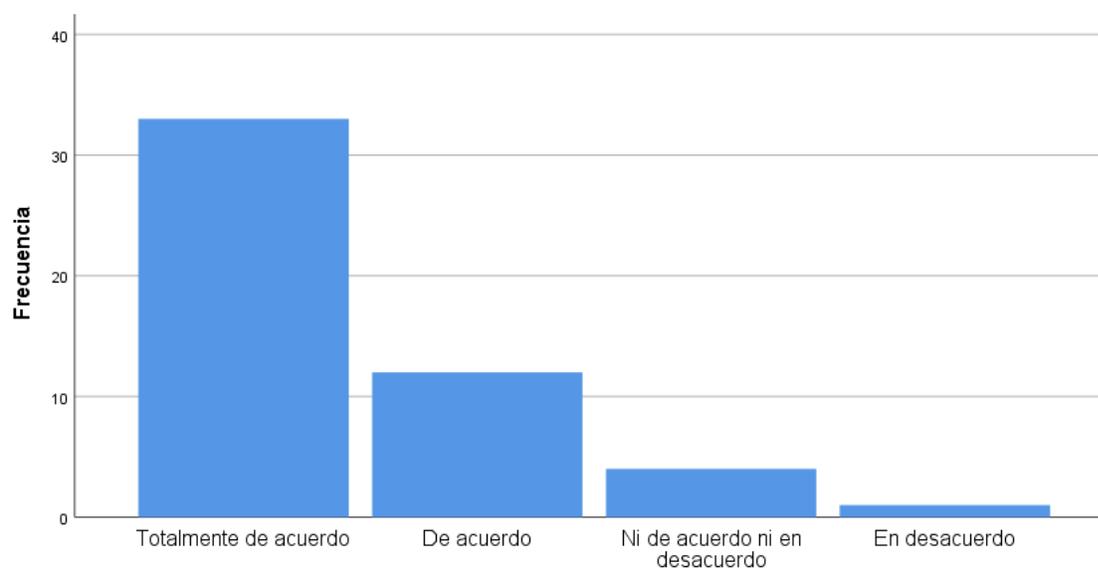


Figura 12: Gráfico de barras de la Pregunta 06: ¿Está usted de acuerdo en que las principales víctimas de estafa son los adultos mayores? Fuente: Elaboración propia – SPSS

De 100 % de colaboradores, un 66 % estuvieron totalmente de acuerdo que las principales víctimas de estafa son los adultos mayores. Por otro lado, para evidenciar los resultados, se puede observar la tabla 9 y figura 12.

Tabla 10

Pregunta 07: ¿Cree usted que los hackers logran su objetivo obteniendo un beneficio ilícito?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
--	------------	------------	-------------------	----------------------

Válido	Totalmente de acuerdo	28	56,0	56,0	56,0
	De acuerdo	12	24,0	24,0	80,0
	Ni de acuerdo ni en desacuerdo	10	20,0	20,0	100,0
	Total	50	100,0	100,0	

Fuente: *Elaboración propia - SPSS*

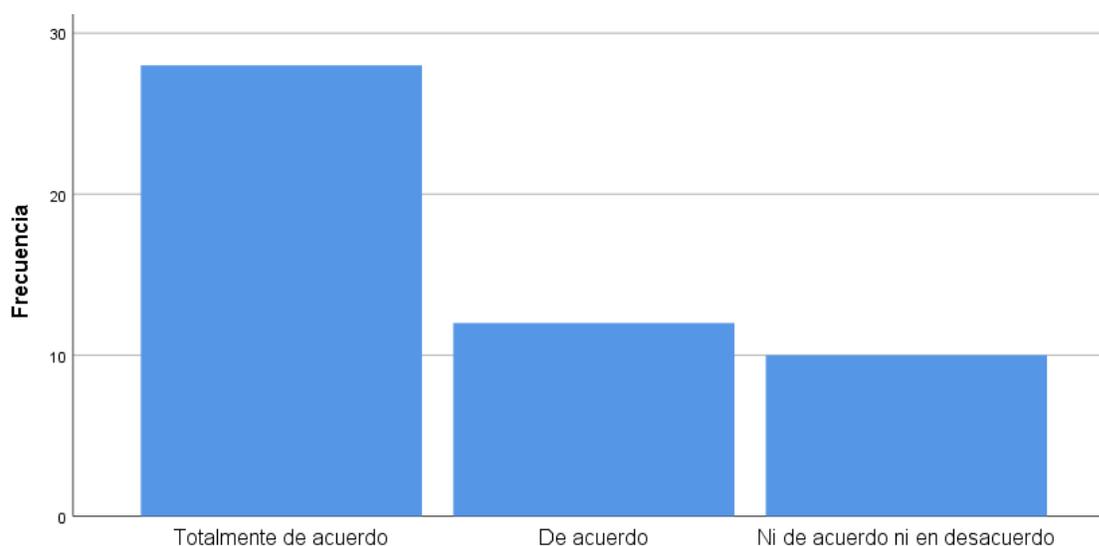


Figura 13: Gráfico de barras de la Pregunta 07 ¿Cree usted que los hackers logran su objetivo obteniendo un beneficio ilícito? Fuente: *Elaboración propia – SPSS*

Como se aprecia en la tabla 10 y figura 13, se puede observar que 28 participantes estuvieron totalmente de acuerdo que los hackers logran su objetivo obteniendo un beneficio ilícito.

Tabla 11

Pregunta 08: ¿Considera usted que el beneficio ilícito es fundamental para que la organización criminal se mantenga con el tiempo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	39	78,0	78,0	78,0
	De acuerdo	11	22,0	22,0	100,0
	Total	50	100,0	100,0	

Fuente: *Elaboración propia - SPSS*

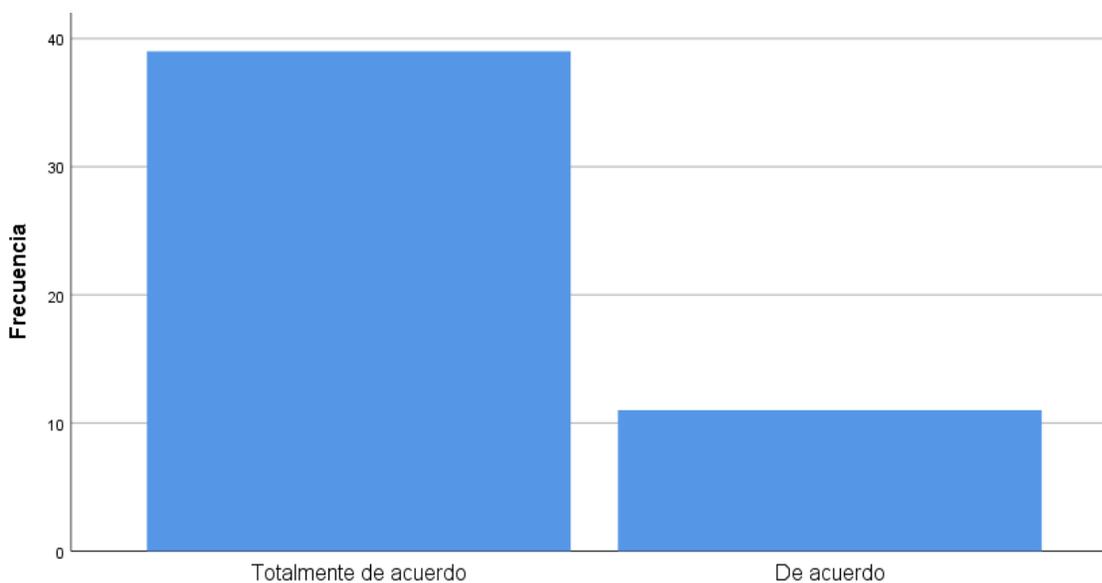


Figura 14: Gráfico de barras de la Pregunta 08 ¿Considera usted que el beneficio ilícito es fundamental para que la organización criminal se mantenga con el tiempo? Fuente: *Elaboración propia – SPSS*

Como se aprecia en la tabla 11 y figura 14, una cifra de 39 participantes estuvieron totalmente de acuerdo que el beneficio ilícito es fundamental para que la organización criminal se mantenga en el tiempo.

Tabla 12

Pregunta 09: ¿Considera usted que la graduación de la pena según el nivel de participación en una organización criminal es aplicable a los delitos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	27	54,0	54,0	54,0
	De acuerdo	23	46,0	46,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

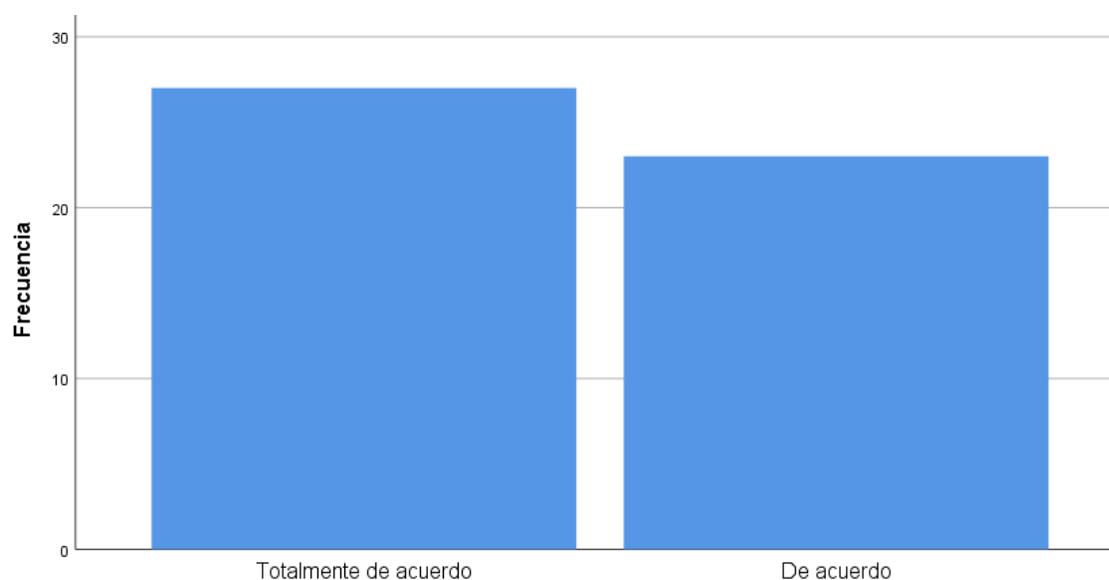


Figura 15: Gráfico de barras de la Pregunta 09. ¿Considera usted que la graduación de la pena según el nivel de participación en una organización criminal es aplicable a los delitos informáticos? Fuente: Elaboración propia – SPSS

Como se aprecia en la tabla 12 y figura 15, del 100 % de encuestados, un 54 % estuvo totalmente de acuerdo que la graduación de la pena según el nivel de participación en una organización criminal es aplicable a los delitos informáticos.

Tabla 13

Pregunta 10: ¿Está usted de acuerdo en que las penalidades de la intervención delictiva necesitan ser actualizadas respecto a los delitos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	28	56,0	56,0	56,0
	De acuerdo	16	32,0	32,0	88,0
	Ni de acuerdo ni en desacuerdo	6	12,0	12,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

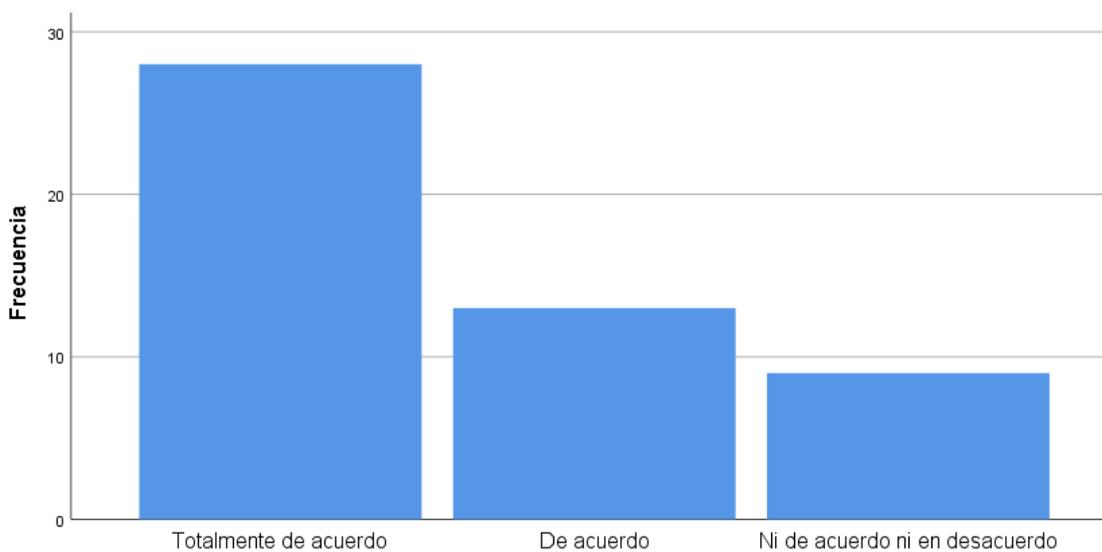


Figura 16: Gráfico de barras de la Pregunta 10. ¿Está usted de acuerdo en que las penalidades de la intervención delictiva necesitan ser actualizadas respecto a los delitos informáticos? Fuente: Elaboración propia – SPSS

Como se aprecia en la tabla 13 y figura 15, se evidencia que 28 colaboradores para obtener resultados verificados, manifestaron estar totalmente de acuerdo que las penalidades de la intervención delictiva necesitan ser actualizadas respecto a los delitos informáticos.

Tabla 14

Pregunta 11: ¿Cree usted que la planificación y repartición de tareas facilita el actuar criminal de las organizaciones criminales?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	38	76,0	76,0	76,0
	De acuerdo	11	22,0	22,0	98,0
	Ni de acuerdo ni en desacuerdo	1	2,0	2,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

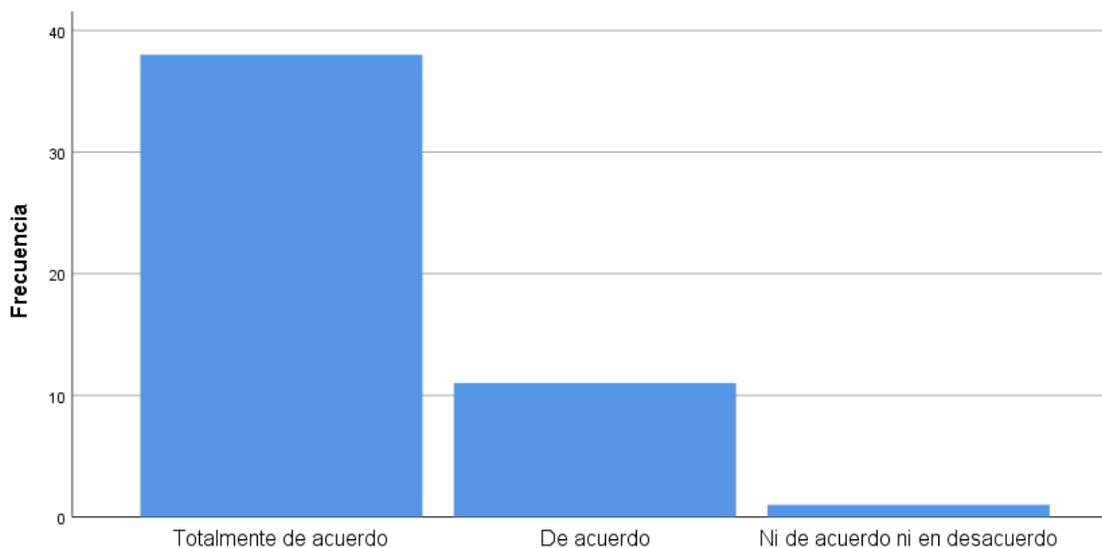


Figura 17: Gráfico de barras de la Pregunta 11. ¿Cree usted que la planificación y repartición de tareas facilita el actuar criminal de las organizaciones criminales? Fuente: Elaboración propia – SPSS

Como se evidencia en la tabla 14 y figura 17, del 100 % de encuestados, un 76 % estuvo totalmente de acuerdo que la planificación y repartición de tareas facilitan el actuar criminal de las organizaciones criminales.

Tabla 15

Pregunta 12: ¿Piensa usted que la planificación y repartición de tareas influyen en la creación de una identidad dentro de la organización criminal?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	37	74,0	74,0	74,0
	De acuerdo	13	26,0	26,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

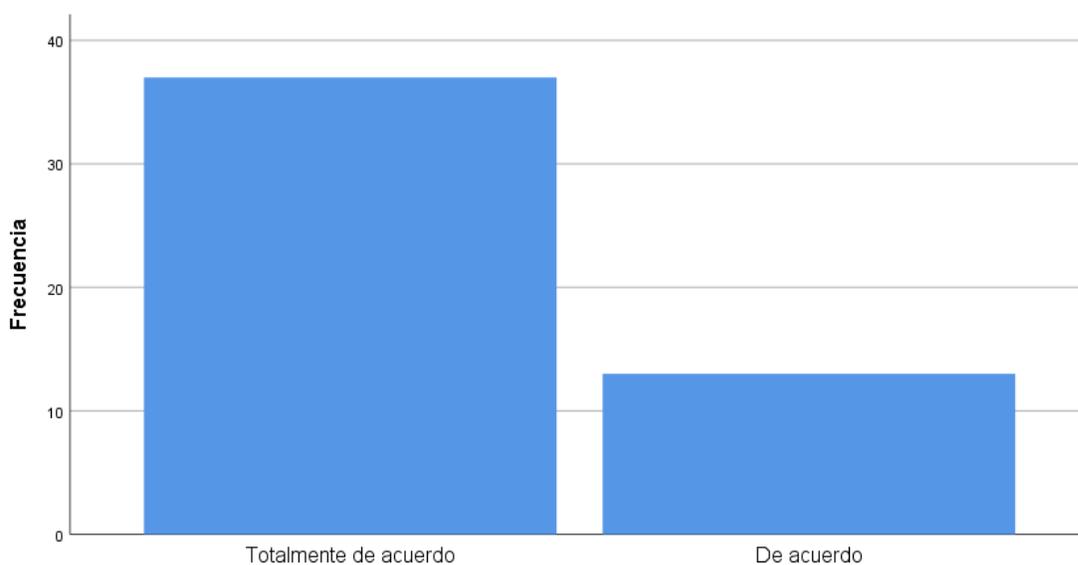


Figura 18: Gráfico de barras de la Pregunta 12. ¿Piensa usted que la planificación y repartición de tareas influyen en la creación de una identidad dentro de la organización criminal? Fuente: Elaboración propia – SPSS

Como se aprecia en la tabla 15 y figura 18, unos 37 colaboradores estuvieron totalmente de acuerdo que la planificación y repartición de tareas influyen en la creación de una identidad dentro de la organización criminal.

Tabla 16

Pregunta 13: ¿Considera usted que las extorsiones delictivas se realizan desde cualquier parte o lugar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	35	70,0	70,0	70,0
	De acuerdo	12	24,0	24,0	94,0
	Ni de acuerdo ni en desacuerdo	3	6,0	6,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

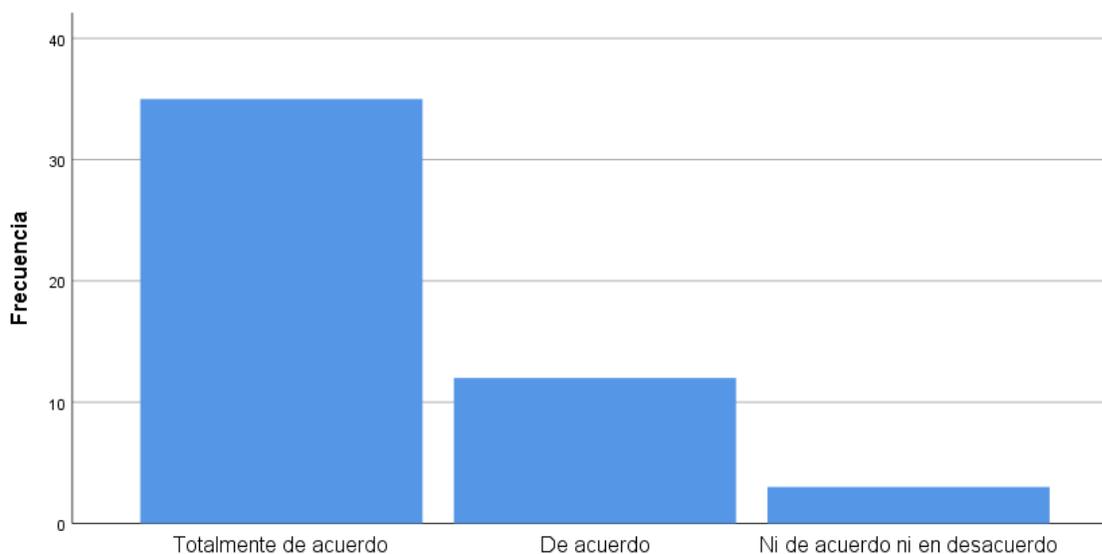


Figura 19: Gráfico de barras de la Pregunta 13 ¿Considera usted que las extorsiones delictivas se realizan desde cualquier parte o lugar? Fuente: Elaboración propia – SPSS

Como se evidencia en la tabla 16 y figura 19, del 100 % de encuestados, un 70 % de ellos estuvieron totalmente de acuerdo que las extorsiones delictivas se realizan desde cualquier parte o lugar.

Tabla 17

Pregunta 14: ¿Cree usted que las extorsiones facilitan la comisión de delitos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	32	64,0	64,0	64,0
	De acuerdo	16	32,0	32,0	96,0
	Ni de acuerdo ni en desacuerdo	2	4,0	4,0	100,0
	Total	50	100,0	100,0	

Fuente: Elaboración propia - SPSS

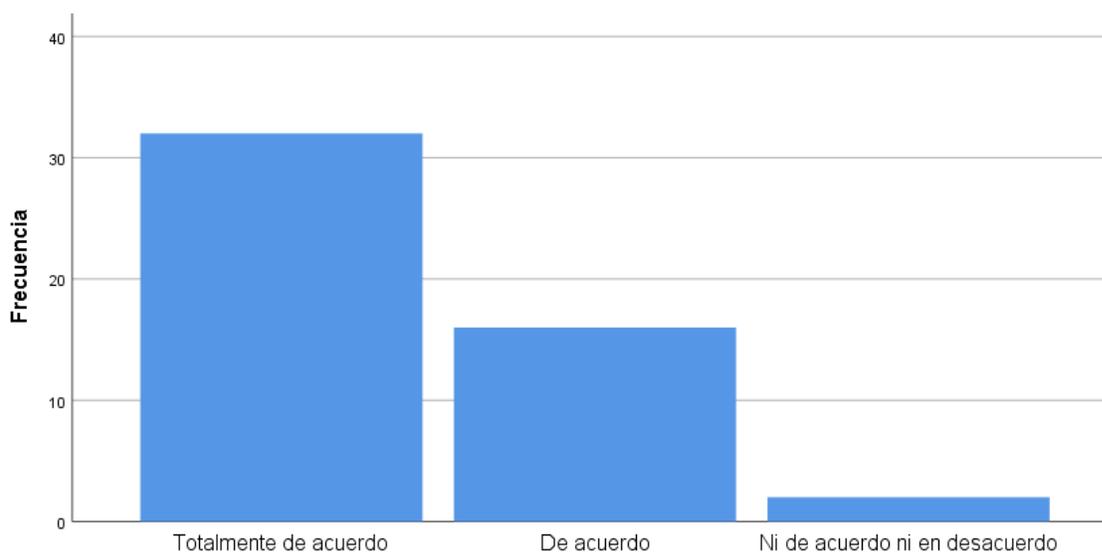


Figura 20: Gráfico de barras de la Pregunta 14: ¿Cree usted que las extorsiones facilitan la comisión de delitos informáticos? Fuente: Elaboración propia – SPSS

Como se aprecia en la tabla 17 y figura 20, se visualiza que del 100 % de colaboradores, un 64 % manifestó estar totalmente de acuerdo que la comisión de los delitos informáticos se facilita gracias a las extorsiones.

Tabla 18

Pregunta 15: ¿Está usted de acuerdo en que la valorización de los beneficios ilícitos afecta en la cantidad de integrantes de un grupo criminal?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	30	60,0	60,0	60,0
	De acuerdo	11	22,0	22,0	82,0
	Ni de acuerdo ni en desacuerdo	9	18,0	18,0	100,0

Total	50	100,0	100,0
-------	----	-------	-------

Fuente: Elaboración propia - SPSS

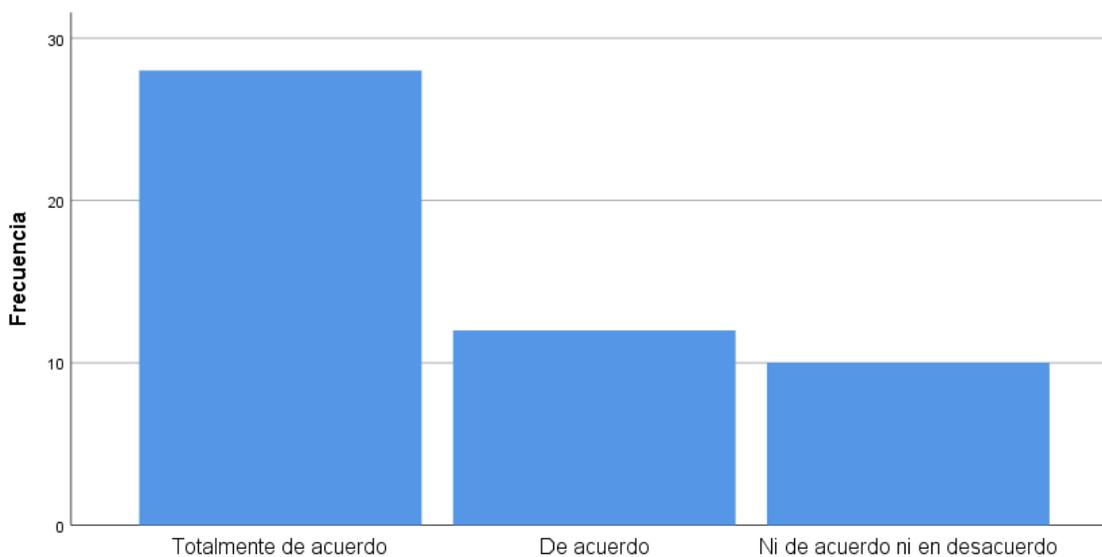


Figura 21: Gráfico de barras de la Pregunta 15. ¿Está usted de acuerdo en que la valorización de los beneficios ilícitos afecta a la cantidad de integrantes de un grupo criminal? Fuente: Elaboración propia – SPSS

Como se aprecia en la tabla 18 y figura 21, del 100 % de encuestadores, un 60 % coincidió estar totalmente de acuerdo en que la valorización de los beneficios ilícitos afecta en la cantidad de integrantes de un grupo criminal.

Tabla 19

Pregunta 16: ¿Piensa usted que no se les juzga a los grupos criminales como se debería en el tema de delitos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente de acuerdo	38	76,0	76,0	76,0
	De acuerdo	12	24,0	24,0	100,0

Total	50	100,0	100,0
-------	----	-------	-------

Fuente: *Elaboración propia - SPSS*

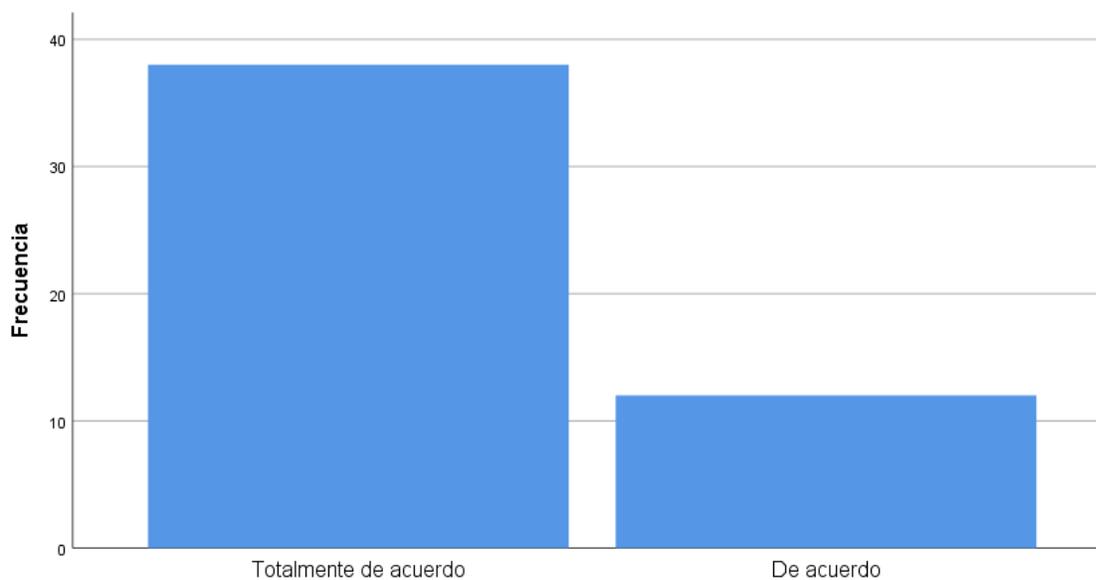


Figura 22: Gráfico de barras de la Pregunta 16. *¿Piensa usted que no se les juzga a los grupos criminales como se debería?* Fuente: *Elaboración propia – SPSS*

Como se aprecia en la tabla 19 y figura 22, de 50 colaboradores, 38 de ellos coincidieron estar totalmente de acuerdo que no se les juzga a los grupos criminales como se debería en el tema de delitos informáticos.

4.1.2. Correlación.

4.1.2.1. Prueba de hipótesis general.

Tabla 20

Correlaciones entre las variables Delitos informáticos y Crimen organizado

		Delitos Informáticos	Crimen Organizado
Delitos Informáticos	Correlación de Pearson	1	,921**
	Sig. (bilateral)		,000
	N	50	50
Crimen Organizado	Correlación de Pearson	,921**	1
	Sig. (bilateral)	,000	
	N	50	50

** . La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia - SPSS

H₁: Hipótesis planteada por el investigador.

H₀: Hipótesis Nula.

- H₁: Los delitos informáticos influyen en el crimen organizado en el distrito de San Isidro – 2020.
- H₀: Los delitos informáticos NO influyen en el crimen organizado en el distrito de San Isidro – 2020.

Como se visualiza en la tabla 20, respecto a la correlación de Pearson $r = 0.921$, esta cifra expresa que existe una correlación muy alta por estar próximo al 1. Asimismo, representa características positivas. Por lo tanto, se valida la hipótesis planteada por el investigador H₁: Los delitos informáticos influyen en el crimen organizado en el distrito de San Isidro – 2020. Esta

aceptación se refleja en que $0.01 > 0.000$ y además por el valor obtenido $r=0.921$ podemos afirmar que la correlación es muy alta.

4.1.2.2. Prueba de hipótesis específicas.

Tabla 21

Correlación entre las variables necesidad de modernizar leyes e intervención delictiva

		Necesidad de modernizar leyes	Intervención delictiva
Necesidad de modernizar leyes	Correlación de Pearson	1	,911**
	Sig. (bilateral)		,000
	N	50	50
Intervención delictiva	Correlación de Pearson	,911**	1
	Sig. (bilateral)	,000	
	N	50	50

** . La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia - SPSS

H_1 : Hipótesis planteada por el investigador.

H_0 : Hipótesis Nula.

- H_1 : La necesidad de modernizar leyes influye en la intervención delictiva en el distrito de San Isidro- 2020.
- H_0 : La necesidad de modernizar leyes NO influye en la intervención delictiva en el distrito de San Isidro- 2020.

Como se aprecia en la Tabla 21 y en análisis a la correlación de Pearson $r= 0.911$, este valor expresa una relación muy alta por estar cerca al 1. Por lo tanto, se valida la hipótesis planteada por el investigador H_1 : La necesidad de modernizar leyes influye en la intervención

delictiva en el distrito de San Isidro- 2020. Esta aceptación se refleja en que $0.01 > 0.000$ y además por el valor obtenido $r=0.911$ podemos afirmar que la correlación es muy alta.

Tabla 22

Correlación entre las variables la explotación de datos personales y la planificación.

		Explotación de datos personales	La planificación
Explotación de datos personales	Correlación de Pearson	1	,930**
	Sig. (bilateral)		,000
	N	50	50
La planificación	Correlación de Pearson	,930**	1
	Sig. (bilateral)	,000	
	N	50	50

** . La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia - SPSS

H₁: Hipótesis planteada por el investigador.

H₀: Hipótesis Nula.

- H₁: La explotación de datos personales influye en la planificación en el distrito de San Isidro- 2020.
- H₀: La explotación de datos personales NO influye en la planificación en el distrito de San Isidro- 2020.

Como se aprecia en la Tabla 22 y en análisis a la correlación de Pearson $r= 0.930$ este valor expresa una relación alta por estar cerca al 1. Por lo tanto, se valida la hipótesis aceptación H₁: La

explotación de datos personales influye en la planificación en el distrito de San Isidro- 2020. Se refleja en que $0.01 > 0.000$ y además por el valor obtenido $r=0.930$ podemos afirmar que la correlación es muy alta.

Tabla 23

Correlación entre las variables estafa y extorsiones delictivas

		Estafa	Extorsiones delictivas
Estafa	Correlación de Pearson	1	,936**
	Sig. (bilateral)		,000
	N	50	50
Extorsiones delictivas	Correlación de Pearson	,936**	1
	Sig. (bilateral)	,000	
	N	50	50

** . La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia - SPSS

H_1 : Hipótesis planteada por el investigador.

H_0 : Hipótesis Nula.

- H_1 : La estafa influye en las extorsiones delictivas en el distrito de San Isidro- 2020.
- H_0 : La estafa NO influye en las extorsiones delictivas en el distrito de San Isidro- 2020.

Como se aprecia en la Tabla 23, además el resultado de la correlación de Pearson $r= 0.936$ representa que existe una correlación muy alta por estar cerca al 1. Asimismo, se acepta la hipótesis planteada por el investigador H_1 : La estafa influye en las extorsiones delictivas en el distrito de

San Isidro- 2020. Esta aceptación se refleja en que $0.01 > 0.000$ y además por el valor obtenido $r=0.936$ podemos afirmar que la correlación es muy alta.

Tabla 24

Correlación entre las variables beneficio ilícito y grupos criminales

		Beneficio ilícito	Grupos Criminales
Beneficio Ilícito	Correlación de Pearson	1	,925**
	Sig. (bilateral)		,000
	N	50	50
Grupos Criminales	Correlación de Pearson	,925**	1
	Sig. (bilateral)	,000	
	N	50	50

** . La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración propia - SPSS

H₁: Hipótesis planteada por el investigador.

H₀: Hipótesis Nula.

- H₁: El beneficio ilícito influye en los grupos criminales en el distrito de San Isidro- 2020.
- H₀: El beneficio ilícito NO influye en los grupos criminales en el distrito de San Isidro- 2020.

Como se aprecia en la Tabla 24, el análisis de la correlación de Pearson $r= 0.925$ presentado así características positivas. Además, se valida la hipótesis planteada por el investigador H_1 : El beneficio ilícito influye en los grupos criminales en el distrito de San Isidro - 2020. Esta aceptación se refleja en que $0.01 > 0.000$ y además por el valor obtenido $r=0.925$ podemos afirmar que la correlación es muy alta.

4.2 Discusión

En una de sus conclusiones, Castañeda (2016) destaca “La represión penal del crimen organizado: Estrategias metodológicas para judicializar graves violaciones a los derechos humanos” explica que el delito de crimen organizado puede darse de 3 formas: convencional, política e internacional. Informa también que a pesar que el 76% de informes de la Defensoría Pública de Colombia tiene como principales actores las bandas criminales aún no existe un mecanismo político judicial, concordando con los resultados de nuestra investigación donde el 76% también está totalmente de acuerdo en que no se les juzga a los grupos criminales como se debería en el tema de delitos informáticos.

En su publicación “El engaño concluyente en el delito de estafa” (Lux, 2014) se explica que el fraude o la estafa es una acción delictiva que se basa en la mentira, información falsa y la confusión continua del proceso que desea lograr el delincuente hacia la víctima, esta modalidad consta de un plan elaborado cautelosamente, para evitar una filtración o apariencia de trampa. La mayoría de las situaciones de estafa se centran en el daño económico del perjudicado, algo que también se refleja en nuestra investigación donde un 54% está totalmente de acuerdo en que el principal delito que se da es el de estafa.

En su tesis “Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016” (Alarcón Ariza & Antonio, 2017), declara que uno de los riesgos que se genera con el uso de internet son los delitos informáticos los cuales afectan la confiabilidad e integridad de la información y que por ende es necesario se empiecen a elaborar capacitaciones con respecto a seguridad informática lo que concuerda con nuestra investigación en donde el 56% está totalmente de acuerdo que la explotación de datos personales ocurre porque muchas personas no tienen el conocimiento sobre medidas de seguridad en los sistemas informáticos de acuerdo sobre los hackers.

Conclusiones:

Como primera conclusión se demostró científicamente a través de una correlación de Pearson, que los delitos informáticos influyen en el crimen organizado en San Isidro. El resultado de esta correlación r fue de 0.921 el mismo que por ser positivo da cuenta de una relación directamente proporcional, al estar cerca al uno se puede considerar como una correlación muy alta. Esto quiere decir que mientras mayor sea la complejidad de los delitos informáticos, más estructurado será el crimen organizado.

Se determinó que la necesidad de modernizar las leyes influye en la intervención delictiva, esto se corroboró con una correlación de Pearson cuyo resultado fue de 0.911, la misma que es considerada una correlación muy alta al estar cerca del uno, además de ser positiva por lo cual es directamente proporcional. De este resultado se puede concluir que la actualización de las leyes referentes a los delitos informáticos generará que la intervención delictiva en el crimen organizado tenga una mejor aplicación en la pena de acuerdo al nivel de participación dentro de la organización criminal.

La explotación de datos personales influye en la planificación, esto se explica con un $r=0.930$ y podemos afirmar que existe una correlación muy alta por estar cerca al número 1 además de haber una relación directamente proporcional por ser positiva. Mientras mayor sea la explotación de datos, mejor será la planificación en las organizaciones criminales.

Asimismo, se comprobó que la estafa influye en las extorsiones delictivas con un $r=0.936$ la cual es una correlación muy alta y además positiva lo cual evidencia una relación directamente proporcional. Mientras las estafas en línea aumentan en esta época de pandemia en que las personas

pasan la mayor parte del tiempo navegando en internet, las extorsiones también van en aumento: extorsiones por estafa romántica o de confianza, extorsiones sexuales, falso servicio.

Finalmente, se corroboró que el beneficio ilícito influye en los grupos criminales con un $r=0.925$ lo cual representa una correlación muy alta además de una relación directamente proporcional. A mayor beneficio ilícito del crimen electrónico, mayor será el aliciente para la transnacionalidad de los grupos criminales.

Recomendaciones:

La primera recomendación en la presente investigación es capacitar al personal encargado de las investigaciones criminales respecto a los avances tecnológicos actuales y las nuevas modalidades de delincuencia informática a nivel mundial. Asimismo, realizar campañas informativas para los ciudadanos del distrito de San Isidro sobre las nuevas modalidades de delincuencia informática y como evitarlas y/o combatirlas.

La segunda recomendación corresponde a la actualización de la normatividad referente a los delitos informáticos. Las autoridades de la municipalidad de San Isidro deben realizar una solicitud de revisión de los últimos proyectos de ley N° 5630/2020-CR¹ y 4929/2020-CR² referente a modificación de la actual normatividad de delitos informáticos y de la ley contra el crimen organizado para abarcar cualquier tipo de delito informático actual que atente a la seguridad de los ciudadanos, principalmente en el aspecto económico, como lo son los delitos informáticos, que se centra en el robo de dinero cibernético.

La Municipalidad y la comisaría de San Isidro, deberían realizar capacitaciones a su personal, referente a los temas de Explotación de datos, Big Data y seguridad de la Información, así como realizar campañas preventivas sobre la adecuada autorización y protección de datos personales dirigidas a los ciudadanos, para evitar que sean víctimas del robo de datos personales a través de las redes sociales, o que sean compartan información privada o excesiva por paginas públicas.

¹ PL05630:
https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL05630-20200625.pdf

² PL04929:
https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL04929_20200326.pdf

Alertar a la ciudadanía de San Isidro, respecto a las nuevas estafas por internet que dan pie a una posterior extorsión, así como de los medios de contacto para denunciar en caso de ser víctima de ellas o solicitar apoyo antes de consumarse la extorsión.

Revisar el “convenio sobre la ciberdelincuencia” de Budapest de fecha 23 de noviembre del 2001, así como la “Resolución legislativa N° 30913 Resolución Legislativa que aprueba el convenio sobre la Ciberdelincuencia” para la cooperación internacional.

Referencias:

- Alarcón Ariza, D. A., & Antonio, B. B. (2017). "Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.". Lima, Perú. Obtenido de <http://repositorio.uwiener.edu.pe/bitstream/handle/123456789/1630/MAESTRO%20-%20%20Barrera%20Bar%C3%B3n%20%20Javier%20Antonio.pdf?sequence=1&isAllowed=y>
- Arenas, A. (26 de Junio de 2020). "¿Cómo prevenir el fraude cibernético? Obtenido de <https://www.infochannel.info/fico-como-prevenir-el-fraude-cibernetico>
- Bazo Reisman, A. (21 de Diciembre de 2018). "Los Cuellos Blancos del Puerto.Los principales investigados y las medidas que les dictó el Poder Judicial". Lima, Perú. Obtenido de <https://rpp.pe/politica/judiciales/los-cuellos-blancos-del-puerto-los-principales-investigados-y-las-medidas-que-les-dicto-el-poder-judicial-noticia-1169624>
- Calderón Martínez, A. (2017). "Teoría del delito y juicio oral. Juicios Orales número 23, 2a. reimp.". Ciudad de México, México. Obtenido de <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3982/4.pdf>
- Carranza Figón, L. (2017). "Crimen organizado corporativo". Barcelona, España. Obtenido de https://www.tesisenred.net/bitstream/handle/10803/471513/LCF_TESIS.pdf?sequence=1&isAllowed=y
- Castañeda Díaz, A. (18 de Julio de 2016). "La represión penal del crimen organizado: Estrategias metodológicas para judicializar graves violaciones a los derechos humanos". Colombia.

Obtenido de

<https://repository.usta.edu.co/bitstream/handle/11634/3403/Castanedaagosto2016.pdf?sequence=1&isAllowed=y>

Chauca Acero, G. C. (2014). "El principio de proporcionalidad en la prevención de los delitos informáticos". Ibarra, Ecuador. Obtenido de

<http://dspace.uniandes.edu.ec/bitstream/123456789/2133/1/TUIAB037-2015.pdf>

Chávez Rodríguez, E. G. (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". Lima, Perú. Obtenido de

<http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y>

Chávez Rodríguez, E. G. (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".

Lima, Perú. Obtenido de

<http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y>

Congreso de la República del Perú. (2013). "Ley N° 30077 - Ley contra el Crimen Organizado".

Lima, Perú. Obtenido de

https://cdn.www.gob.pe/uploads/document/file/225388/Ley_30077_Ley_contra_el_Crimen_Organizado.pdf

- Congreso de la República del Perú. (Marzo de 2014). "Ley de Delitos Informáticos - LEY N° 30171". Lima, Perú. Obtenido de https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/02/Ley_30096.pdf
- Cordini, N. S. (Abril de 2017). "El crimen organizado: un concepto extraño al derecho penal argentino". Buenos Aires, Argentina. Obtenido de https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322017000100344
- Córdoba Moreno, S. (2015). "La delincuencia organizada y su prevención. Especial referencia a las pandillas latinoamericanas de tipo violento". Salamanca, España. Obtenido de https://gedos.usal.es/bitstream/handle/10366/128112/DDPG_C%F3rdobaMorenoS_Delincuenciorganizadaprevenci%F3n.pdf;jsessionid=F8682465E0669D969010F00168ED2ED8?sequence=1
- Couso, J. (2015). Intervención delictiva y organización. Necesidad y complejidades de una comparación funcional entre el derecho chileno y el derecho internacional y comparado. *Revista chilena de derecho*. Chile: Google Chrome. Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-34372015000100011
- Diario El País. (29 de Junio de 2018). "Las rutas de distribución de la cocaína en el mundo". España. Obtenido de https://elpais.com/elpais/2018/06/29/media/1530279984_222697.html
- Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. d. (2014). *Metodología de la investigación*. México: Mc Graw Hill.

Hurtado Paico, J. (30 de Octubre de 2018). "¿En qué consiste una organización criminal y cómo opera la imputación de responsabilidad a sus miembros?". Lima, Perú. Obtenido de https://lpderecho.pe/organizacion-criminal-imputacion-responsabilidad-miembros/#_ftnref9

Hurtado Paico, J. (Octubre de 2018). "¿En qué consiste una organización criminal y cómo opera la imputación de responsabilidad a sus miembros?". Lima, Perú. Obtenido de <https://lpderecho.pe/organizacion-criminal-imputacion-responsabilidad-miembros/>

Jiménez Serrano, J. (2015). "Crimen organizado: una aproximación al fenómeno". España. Obtenido de https://www.uv.es/gicf/4A3_Jimenez_GICF_14.pdf

Llinares, F. M. (2013). La respuesta penal al ciberfraude, especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*. España: Google Chrome.

López Mendoza, F. (Junio de 2018). "Alternativa para mejorar el proceso de investigación que contribuya a la reducción del accionar del crimen organizado tomando en cuenta la técnica especial de investigación de agente encubierto". Lima, Perú. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/13492/LOPEZ_MENDOZA_FREDY.pdf?sequence=6&isAllowed=y

López Vargas, J. A., & Milagro, T. G. (Junio de 2010). "Problemática del Delito Informático: Hacia una necesaria regulación internacional.". Costa Rica. Obtenido de <https://ijj.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/PROBLEMATICA-DEL-DELITO-INFORMATICO.pdf>

Lux, L. M. (2014). El engaño concluyente en el delito de estafa. *Revista chilena de derecho*.

Chile: Google Chrome. Obtenido de

https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-34372014000300010

Martínez Martínez, J. (2015). "Estrategias multidisciplinares de seguridad para prevenir el crimen organizado". Barcelona, España. Obtenido de

<https://www.tdx.cat/bitstream/handle/10803/298308/jmm1de1.pdf?1>

Martínez Martínez, J. (2015). "Estrategias multidisciplinares de seguridad para prevenir el crimen organizado". Barcelona, España. Obtenido de

<https://www.tdx.cat/bitstream/handle/10803/298308/jmm1de1.pdf?1>

Mendonça, A. L. (2016). Los criterios para la mensuración del valor del enriquecimiento ilícito y perjuicios causados por actos corruptos. *Revista da AGU*. Brasil: Google Chrome.

Obtenido de

<https://pdfs.semanticscholar.org/e53f/0979c7e07329158da374d7a96ef6aec0b8e3.pdf>

Mesa Pinedo, M. M. (2018). "Globalización y transnacionalización de la violencia en Centroamérica: los países del Triángulo Norte". Madrid, España. Obtenido de

<https://eprints.ucm.es/49575/1/T40373.pdf>

Ministerio de Justicia y Derechos Humanos. (Mayo de 2016). Decreto Legislativo N° 635 - Código Penal Décimo Segunda Edición. Lima, Perú. Obtenido de

http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf

Ministerio del Interior del Perú. (Noviembre de 2019). "Política Nacional Multisectorial de lucha contra el Crimen Organizado 2019 - 2030". Lima, Perú. Obtenido de https://cdn.www.gob.pe/uploads/document/file/473340/PLC_MININTER.pdf

Morales Delgado, D. Y. (Abril de 2016). "La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015". Perú. Obtenido de http://repositorio.uss.edu.pe/bitstream/handle/uss/3161/MORALES_DELGADO_DEIVI_D_1%20YULY-1.%20turnitin.pdf?sequence=6&isAllowed=y

Portilla Marzano, F., & Taboada Cárdenas, A. L. (4 de Junio de 2020). "Los delitos informáticos en tiempos de e-commerce". Lima, Perú. Obtenido de <https://ius360.com/publico/penal/los-delitos-informaticos-en-tiempos-de-e-commerce-fernando-portilla-ana-lucia-taboada/>

Quevedo González, J. (2017). "Investigación y prueba del Cibercrimen". Barcelona, España. Obtenido de https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Quintana Salazar, D. (Septiembre de 2015). "El papel de la Policía Federal Ministerial en el combate al crimen organizado en Tijuana, durante el periodo 2006 - 2014". Toluca, México. Obtenido de <https://core.ac.uk/download/pdf/80533512.pdf>

Riquelme Rivera, J., Salinas Cañas, S., & Franco Severino, P. (Diciembre de 2018). "El Crimen Organizado Transnacional (COT) en América del Sur. Respuestas regionales". Obtenido de <https://revistaei.uchile.cl/index.php/REI/article/view/52781/55775#info>

Ruiz Ramal, A. (2016). "Los delitos culposos". Lima, Perú. Obtenido de

<http://revistas.urp.edu.pe/index.php/Inkarri/article/download/541/543/>

Sánchez Velasco, A., Galicia Moyeda, I. X., & Robles Ojeda, F. J. (Enero de 2017). "Conductas antisociales-delictivas en adolescentes: relación con el género, la estructura familiar y el rendimiento académico". Ciudad de México, México. Obtenido de

https://alternativas.me/27-numero-38-agosto-2017-enero-2018/158-conductas-antisociales-delictivas-en-adolescentes-relacion-con-el-genero-la-estructura-familiar-y-el-rendimiento-academico#_ftn1

Scheller D'angelo, A., & Lugo Quiroz, E. d. (13 de Mayo de 2019). "Conceptualización del Crimen Organizado y su regulación en la legislación Penal Colombiana". Obtenido de

http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20190808_01.pdf

Suárez Sánchez, A. (2009). *"La estafa informática"*. Bogotá, Colombia: Bogotá: Ibáñez.

Sucari Ccopacondori, S. G. (2015). "Control de la criminalidad organizada y aplicación en el sistema jurídico penal peruano". Puno, Perú. Obtenido de

http://repositorio.unap.edu.pe/bitstream/handle/UNAP/9582/Stip_Gonzalo_Sucari_Ccopacondori.pdf?sequence=1&isAllowed=y

Tokatlian, J. G. (2015). "La Argentina y las etapas del narcotráfico". Obtenido de

<https://www.lanacion.com.ar/opinion/la-argentina-y-las-etapas-del-narcotrafico-nid1663038/>

Torres, J. M. (Enero de 2016). "Criminalidad Organizada en el Perú: Narcotráfico, Corrupción y otros delitos". Lima, Perú. Obtenido de <http://www.red-alas.net/wordpress/wp-content/uploads/2016/02/Criminalidad-Organizada-en-el-Peru%CC%81-Torres-VF.pdf>

Tumi Pacori, R. E. (Junio de 2020). "¿Cuáles son las diferencias entre banda criminal y organización criminal?". Lima, Perú. Obtenido de <https://lpderecho.pe/diferencias-entre-banda-criminal-organizacion-criminal/>

UNODC. (2020). "Crimen Organizado Transnacional". Obtenido de <https://www.unodc.org/ropan/es/organized-crime.html>

Valgañón, M., Muños, L., & Briccola, M. (2014). "La reiterancia de la conducta delictiva en adolescentes y su relación con las representaciones sociales acerca del rol ejercido por las madres". Chile. Obtenido de http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S0718-74752014000100005#1

Villavicencio Terreros, F. (2015). "Delitos Informáticos". Obtenido de <http://revistas.pucp.edu.pe/index.php/iusetveritas/article/download/13630/14253/>

Anexo N° 01: Matriz de consistencia

Título: “La influencia de los delitos informáticos con respecto al crimen organizado en el distrito de San Isidro– 2020”.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES E INDICADORES	DIMENSIONES
<p>PROBLEMA PRINCIPAL</p> <p>¿Cuál es la influencia de los delitos informáticos con respecto al crimen organizado en el distrito de San isidro - 2020?</p> <p>PROBLEMAS ESPECÍFICOS</p> <p>1. ¿Cómo influye la necesidad de modernizar las leyes en la intervención delictiva del crimen organizado en el distrito de San Isidro - 2020?</p> <p>2. ¿De qué forma la explotación de datos personales influye en la planificación de las organizaciones criminales en el distrito de San Isidro - 2020?</p> <p>3. ¿De qué forma la estafa influye en las extorsiones delictivas transnacionales del crimen organizado en el distrito de San Isidro- 2020?</p>	<p>OBJETIVO GENERAL</p> <p>Determinar la influencia de los delitos informáticos dentro del crimen organizado en el distrito de San Isidro - 2020</p> <p>OBJETIVOS ESPECÍFICOS</p> <p>1. Analizar la influencia de la necesidad de modernizar las leyes en la intervención delictiva del crimen organizado en el distrito de San Isidro- 2020.</p> <p>2. Detallar la influencia de la explotación de datos personales en la planificación de las organizaciones criminales en el distrito de San Isidro - 2020</p> <p>3. Establecer la influencia de la estafa en las extorsiones delictivas transnacionales del crimen organizado en el distrito de San Isidro- 2020.</p> <p>4. Mencionar la influencia del beneficio ilícito en los grupos</p>	<p>HIPÓTESIS GENERAL</p> <p>Los delitos informáticos influyen en el crimen organizado en el distrito de San Isidro - 2020</p> <p>HIPÓTESIS SECUNDARIAS</p> <p>1. La necesidad de modernizar leyes influye en la intervención delictiva del crimen organizado en el distrito de San Isidro- 2020</p> <p>2. La explotación de datos personales influye en la planificación de las organizaciones criminales en el distrito de San Isidro - 2020.</p> <p>3. La estafa influye en las extorsiones delictivas transnacionales del crimen organizado en el distrito de San Isidro- 2020.</p> <p>4. El beneficio ilícito influye en los grupos criminales transnacionales del crimen organizado en el distrito de San Isidro- 2020.</p>	<p>VARIABLE INDEPENDIENTE (X-1):</p> <p>Delitos Informáticos</p> <p>INDICADORES:</p> <p>1. Necesidad de modernizar leyes</p> <p>2. Explotación de datos personales</p> <p>3. Estafa</p> <p>4. Beneficio ilícito</p> <p>VARIABLE DEPENDIENTE (Y -2):</p> <p>Crimen Organizado</p> <p>INDICADORES:</p> <p>1. Intervención delictiva</p> <p>2. Planificación</p> <p>3. Extorsiones delictivas</p> <p>4. Grupos criminales</p>	<p>DIMENSIONES DE LOS DELITOS INFORMÁTICOS:</p> <p>1. Conductas maliciosas</p> <p>2. Crimen electrónico</p> <p>DIMENSIONES DEL CRIMEN ORGANIZADO:</p> <p>1. Jerarquía estructurada</p> <p>2. Transnacionalidad</p>

4. ¿Cómo el beneficio ilícito influye en los grupos criminales transnacionales del crimen organizado en el distrito de San Isidro- 2020?	criminales transnacionales del crimen organizado en el distrito de San Isidro- 2020.			
--	--	--	--	--

Anexo N° 02: Instrumento de la Investigación

CUESTIONARIO

Título: “La influencia de los delitos informáticos con respecto al crimen organizado en la ciudad de Lima-2020”.
La presente es una encuesta que tiene por finalidad establecer cuál es la influencia de los delitos informáticos respecto al crimen organizado.

Indicaciones:

La presente encuesta es de carácter confidencial, agradecemos responder objetiva y verazmente. Lea detenidamente cada pregunta y marque la opción que considere correspondiente según la siguiente leyenda:

Totalmente de acuerdo 1	De acuerdo 2	No de acuerdo, ni en desacuerdo 3	En desacuerdo 4	Totalmente en desacuerdo 5
----------------------------	-----------------	--------------------------------------	--------------------	-------------------------------

PREGUNTAS	RESPUESTAS				
	1	2	3	4	5
1. ¿Considera usted que es necesario modernizar las leyes debido a que con el paso del tiempo aparecen nuevos delitos?					
2. ¿Está usted de acuerdo en que se deben incorporar más leyes para regular los delitos informáticos?					
3. ¿Cree usted que el mal uso de la explotación de datos personales constituye una grave falta a la integridad de la persona?					
4. ¿Piensa usted que la explotación de datos personales ocurre porque muchas personas no tienen el conocimiento sobre medidas de seguridad en los sistemas informáticos?					
5. ¿Considera usted que el principal objetivo de los delitos informáticos es la estafa?					
6. ¿Está usted de acuerdo en que las principales víctimas de estafa son los adultos mayores?					
7. ¿Cree usted que los hackers logran su objetivo obteniendo un beneficio ilícito?					
8. ¿Considera usted que el beneficio ilícito es fundamental para que la organización criminal se mantenga con el tiempo?					
9. ¿Considera usted que la graduación de la pena según el nivel de participación en una organización criminal es aplicable a los delitos informáticos?					
10. ¿Está usted de acuerdo en que las penalidades de la intervención delictiva necesitan ser actualizadas respecto a los delitos informáticos?					
11. ¿Cree usted que la planificación y repartición de tareas facilita el actuar criminal de las organizaciones criminales?					

12. ¿Piensa usted que la planificación y repartición de tareas influyen en la creación de una identidad dentro de la organización criminal?					
13. ¿Considera usted que las extorsiones delictivas se realizan desde cualquier parte o lugar?					
14. ¿Cree usted que las extorsiones facilitan la comisión de delitos informáticos?					
15. ¿Está usted de acuerdo en que la valorización de los beneficios ilícitos afecta a la cantidad de integrantes de un grupo criminal?					
16. ¿Piensa usted que no se les juzga a los grupos criminales como se debería?					

Anexo N° 03: Instrumento de Validación

INFORME DE OPINIÓN DE EXPERTOS DE INSTRUMENTO DE MEDICIÓN

I. DATOS GENERALES:

- 1.1. Apellidos y nombres del validador: Santamaría Portocarrero, Walter
- 1.2. Grado Académico: Magister en Gestión pública
- 1.3. Institución donde labora:
- 1.3.1. Especialidad del validador: Abogado
- 1.3.2. Título de la investigación: **La influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro-2020.**
- 1.3.3. Autor del Instrumento: **LOURDES MAXIMINA HUARCAYA BORDA**
- 1.3.4 Instrumento:
- ENCUESTA: Cuestionario aplicado a 50 personas que laboran y concurren continuamente a la comisaría de San Isidro.**

ASPECTO GLOBAL DEL INSTRUMENTO

INDICADORES	CRITERIOS	Deficiente	Regular	Buena	Muy Buena	Excelente
		1	2	3	4	5
1. CLARIDAD	Está formulado con lenguaje apropiado, específico y comprensible.				X	
2. OBJETIVIDAD	Está expresado en conductas observables.				X	
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.				X	
4. SUFICIENCIA	Comprende los aspectos en cantidad y calidad				X	
5. ORGANIZACION	Presentación ordenada				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias, los datos permiten un tratamiento estadístico pertinente.				X	
7. CONSISTENCIA	Basado en aspectos teórico-científicos				X	
8. COHERENCIA	Entre los índices, indicadores y las dimensiones.				X	
9. METODOLOGIA	La estrategia responde al propósito del diagnóstico				X	
10. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.				X	

PROMEDIO DE VALORACIÓN: 46 OPINIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

() El instrumento debe ser mejorado antes de ser aplicado.

Lugar y fecha: Lima 09 de noviembre de 2020



DNI. N° 41028327
Teléfono N°

INFORME DE OPINIÓN DE EXPERTOS DE INSTRUMENTO DE MEDICIÓN

II. DATOS GENERALES:

1.4. Apellidos y nombres del validador: Morales Gallo, Martín

1.5. Grado Académico: Maestro

1.6. Institución donde labora: Universidad Peruana de Las Américas

1.6.1. Especialidad del validador: Abogado

1.6.2. Título de la investigación: **La influencia de los delitos informáticos en el crimen organizado en el distrito de San Isidro-2020.**

1.6.3. Autor del Instrumento: **LOURDES MAXIMINA HUARCAYA BORDA**

1.3.4 Instrumento:

ENCUESTA: Cuestionario aplicado a 50 personas que laboran y concurren continuamente a la comisaría de San Isidro.

ASPECTO GLOBAL DEL INSTRUMENTO

INDICADORES	CRITERIOS	Deficiente	Regular	Buena	Muy Buena	Excelente
		1	2	3	4	5
1. CLARIDAD	Está formulado con lenguaje apropiado, específico y comprensible.				X	
2. OBJETIVIDAD	Está expresado en conductas observables.				X	
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.				X	
4. SUFICIENCIA	Comprende los aspectos en cantidad y calidad				X	
5. ORGANIZACION	Presentación ordenada				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias, los datos permiten un tratamiento estadístico pertinente.				X	
7. CONSISTENCIA	Basado en aspectos teórico-científicos				X	
8. COHERENCIA	Entre los índices, indicadores y las dimensiones.				X	
9. METODOLOGIA	La estrategia responde al propósito del diagnóstico				X	
10. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.				X	

PROMEDIO DE VALORACIÓN: 46 OPINIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

() El instrumento debe ser mejorado antes de ser aplicado.

Lugar y fecha: Lima 09 de noviembre de 2020



CAL N° 27518

Anexo N° 04: Ejemplo de campaña para evitar ser víctima de la delincuencia informática.

Sexting

Sonsacamiento de la información publicada

Exigencias económicas a cambio de no difundir **material íntimo** intercambiado.

Creación de perfiles falsos en redes sociales
"GROOMING"

Promesa de trabajo en agencias de modelaje o relaciones amorosas virtuales con intercambio de fotografías y videos íntimos.

Recomendaciones para evitar ser víctima en las redes sociales y sexting

- 1. Nunca publicar** información personal en la redes.
- 2. Tenga precaución con las fotos** y videos que sube a la red, esto habla de su nivel social y sobre todo económico.
- 3. Sea discreto con sus actualizaciones** de estado, donde estudia, que hace su familia, donde trabajan, que bienes o negocios tienen. Lo está
- 4. Evite contacto** con desconocidos a través de las redes sociales.
- 5. No acepte ver o conocer físicamente** a extraños que haya aceptado
- 6. Evite compartir** imágenes y/o videos íntimos con contenido sexual.
- 7. Establezca los parámetros** de privacidad en su red social para que solo las personas que usted desee vean lo que compare.
- 8. Asegúrese de utilizar** contraseñas
- 9. Si su hijo/a posee** redes sociales supervise su utilización.
- 10. En lo posible** tenga conocimiento de la clave que utiliza su hijo en redes sociales con el fin de

165
YO NO PAGO
YO DENUNCIO
GAULA
POLICIA NACIONAL

Anexo N° 05: Extorsión por Estafa Romántica

El Sol de México

EL TIMO DEL COFRE ESPAÑOL

Los defraudadores se reinventan en viejos trucos que, pese al tiempo, les pueden dar resultados, y utilizan para ello redes sociales, donde pueden fabricarse personalidades distintas, con otros nombres y nacionalidades de países lejanos. Incluso utilizan a terceras personas para que les ayuden en la farsa.



1
Los defraudadores toman una personalidad extranjera y conocen a sus posibles víctimas a través de las redes sociales



2
Después de que las tratan por varios meses. Las citan para conocerlas



3
No llegan a la cita, pero después aparece un tercero que pide dinero a nombre del extranjero para sacar de la aduana un paquete con objetos valiosos



elsoldemexico.com.mx

f o v t

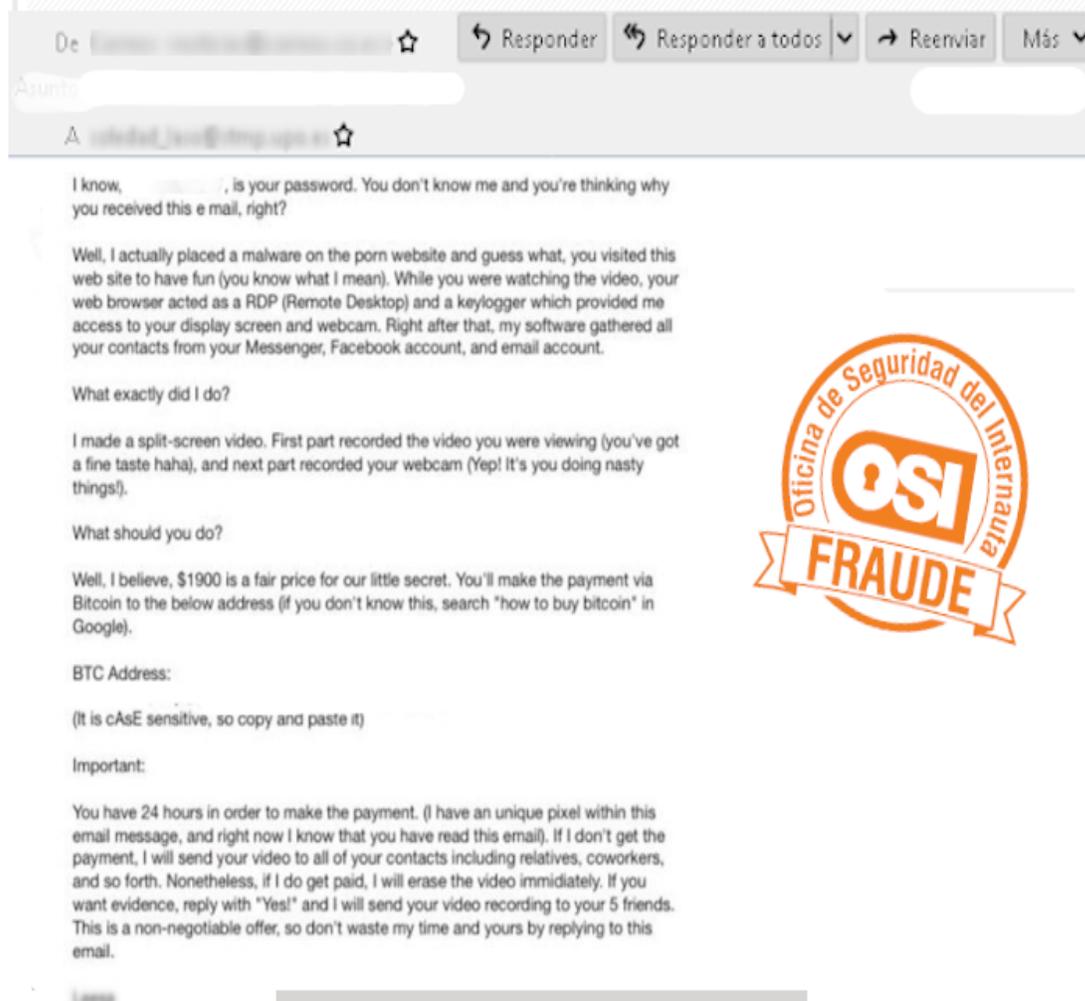
Anexo N° 06: Extorsión sexual

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

“ Nueva oleada de correos electrónicos de sextorsión ”



#OSlavisos

www.incibe.es | www.osi.es

“ Nueva oleada de correos electrónicos de sextorsión ”



xxxxxxx@outlook.com Lets get right to purpose. I know elchamo is your passphrase. Nobody has paid me to check you. You may not know me and you're most likely wondering why you are getting this e-mail? I actually setup a malware on the xxx streaming (sexually graphic) web site and you know what, you visited this website to experience fun (you know what I mean). While you were watching video clips, your internet browser started out operating as a RDP having a keylogger which provided me access to your screen and webcam. Just after that, my software gathered all your contacts from your Messenger, social networks, and email. Next I created a video. First part displays the video you were viewing (you have a good taste hahah), and next part displays the view of your cam, yeah its you. You will have two solutions. Why don't we go through these types of choices in particulars: First choice is to just ignore this e-mail.

In this instance, I am going to send out your videotape to each one of your contacts and also think about the disgrace you will definitely get. Keep in mind if you are in an important relationship, precisely how it will eventually affect? Number 2 solution should be to pay me 1900 USD. We are going to regard it as a donation. As a consequence, I will straight away discard your video footage. You will go forward your daily routine like this never happened and you are never going to hear back again from me. You'll make the payment by Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google).

βTC Address: [redacted] case-SENSITIVE, copy & paste it]

If you are looking at going to the law enforcement, good, this email can not be traced back to me. I have covered my actions. I am also not attempting to demand a huge amount, I prefer to be compensated. You have one day in order to pay. I have a specific pixel within this e-mail, and now I know that you have read through this e-mail. If I do not receive the bitCoins, I will send out your video to all of your contacts including close relatives, co-workers, and many others.

Nevertheless, if I do get paid, I'll destroy the video immediately. It's a nonnegotiable offer so do not waste my personal time & yours by responding to this mail. If you want to have evidence, reply Yeah! and I definitely will send your video recording to your 6 contacts.

#OSlavisio

www.incibe.es | www.osi.es





Campaña de sextorsión, ahora, en español

De [Estimado usuario@correo.com](#) ☆ Responder Responder a todos Reenviar Más

A [usuario_usuario@correo.com](#) ☆

iHola!

Soy un hacker que tiene acceso a su sistema operativo.
También tengo pleno acceso a su cuenta.
Llevo observándole desde hace unos meses.
Su equipo se infectó con un malware cuando visitó un sitio web para adultos.
Se lo explicaré mejor por si no está familiarizado con este tema.
El troyano me da acceso y control total sobre el ordenador o cualquier otro dispositivo.
Esto significa que puedo ver todo lo que aparece en su pantalla y encender la cámara y el micrófono sin que usted se de cuenta.
También tengo acceso a todos sus contactos y mensajes.
¿Por qué su antivirus no detecta el malware?
Respuesta: mi malware dirige el controlador y actualizo sus firmas cada 4 horas para que el antivirus se mantenga en silencio.
He grabado un vídeo en el que sale usted satisfaciéndose en la parte izquierda de la pantalla y en la parte derecha se puede ver el vídeo que está mirando.
Con un solo clic puedo enviar este vídeo a todos sus contactos de correo electrónico y de las redes sociales.
También puedo publicar el acceso en todos sus mensajes de correos electrónico y de messenger.
Si quiere evitarlo,
transfiera 1000 \$ a mi dirección bitcoin (si no sabe cómo hacerlo, escriba en Google: "Comprar bitcoins").
Mi dirección bitcoin (monedero de bitcoin) es: xxxxxxxxxxxxxxxvGCHxxxxxxxxvJBww
Una vez que haya recibido el pago, borraré el vídeo y no volverá a saber nada de mí.
Le doy 50 horas (más de 2 días) para pagar.
Cuando lea esta carta recibirá un aviso y el temporizador se pondrá en marcha.
Presentar una denuncia no tiene sentido porque este correo electrónico no puede ser rastreado, al igual que mi dirección bitcoin.
Yo no cometo errores.
Si descubro que ha compartido este mensaje con alguien más, el vídeo se distribuirá inmediatamente.

iUn saludo!



#OSlavisio

www.incibe.es | www.osi.es

Anexo N° 06: correos de extorsión dirigidos a empresas



INSTITUTO NACIONAL DE CIBERSEGURIDAD



017
PLAN NACIONAL DE
CIBERSEGURIDAD



protege
tu empresa

Nombre [REDACTED]
Email [REDACTED]
Consulta ¿ENVÍE ESTE CORREO ELECTRÓNICO A ALGUIEN DE SU EMPRESA QUE PUEDA TOMAR DECISIONES IMPORTANTES!

Hemos pirateado su sitio web [REDACTED] y extraído sus bases de datos.

¿Cómo pasó esto?
 Nuestro equipo ha encontrado una vulnerabilidad dentro de su sitio que pudimos explotar. Después de encontrar la vulnerabilidad, pudimos obtener las credenciales de su base de datos, extraer toda su base de datos y trasladar la información a un servidor offshore.

¿Qué significa esto?
 Realizaremos sistemáticamente una serie de pasos para dañar totalmente su reputación. Primero, toda su base de datos se filtrará o se venderá al mejor postor que utilizará con cualquiera que sea su intención. A continuación, si se encuentran correos electrónicos, se les enviará por correo electrónico que su información se ha vendido o filtrado y su sitio y teniendo clientes / asociados enojados con cualquier enojo cliente / asociados lo hacen. Por último, los enlaces que haya indexado en los motores de búsqueda se desindexarán en función de las técnicas de backhat que utilizamos en el pasado para desindexar nuestros objetivos.

¿Cómo paro esto?
 Estamos dispuestos a abstenemos de destruir la reputación de su sitio por una pequeña suma su tarifa actual es de .321 BTC en bitcoins (\$ 3000 USD). Envíe el bitcoin a la siguiente dirección de bitcoin (copie y pegue ya que distingue entre mayúsculas y minúsculas):

Una vez que haya pagado, nos informará inmediatamente de que se hizo su pago. Tenga en cuenta que debe realizar el pago dentro de los 5 días posteriores a la recepción de este correo electrónico de la base de datos, los correos electrónicos enviados y la eliminación del índice de su sitio COMENZARÁN

¿Cómo obtengo Bitcoins?
 Puede comprar fácilmente bitcoins a través de varios sitios web o incluso fuera de línea desde un cajero automático de Bitcoin. Le sugerimos <https://cex.io/> para comprar bitcoins.

¿Qué pasa si no pago?
 Si decide no pagar, comenzaremos el ataque en la fecha indicada y lo mantendremos hasta que lo haga, no hay contramedida para esto, solo terminará desperdiciando más dinero tratando de encontrar una solución. Destruiremos por completo su reputación entre Google y sus clientes.

Esto no es un engaño, no responda a este correo electrónico, no intente razonar o negociar, no leeremos ninguna respuesta. Una vez que haya pagado, dejaremos de hacer lo que estábamos haciendo y nunca más volverá a saber de nosotros. Tenga en cuenta que Bitcoin es anónimo y nadie se dará cuenta de que ha cumplido.

www.incibe.es/protege-tu-empresa

Anexo N° 07: Resolución legislativa N° 30913

LEGALES

Miércoles 13 de febrero de 2019 /  El Peruano

- exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad.
- b. De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático.
 - c. De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal.
 - d. De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el literal e) del numeral 9 del citado artículo del Convenio deberán dirigirse a su autoridad central.

RESERVAS

- a. De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio.
- b. De conformidad con el numeral 4 del artículo 9 del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad.
- c. Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal.

1740637-1

RESOLUCIÓN LEGISLATIVA N° 30913

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Resolución Legislativa siguiente:

RESOLUCIÓN LEGISLATIVA QUE APRUEBA EL CONVENIO SOBRE LA CIBERDELINCUENCIA

Artículo Único. Aprobación del Convenio

Apruébase el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001, con las siguientes declaraciones y reservas:

DECLARACIONES

- a. De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los cuatro días del mes de febrero de dos mil diecinueve.

DANIEL SALAVERRY VILLA
Presidente del Congreso de la República

LEYLA CHIHUÁN RAMOS
Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE DE LA REPÚBLICA

Lima, 12 de febrero de 2019.

Cúmplase, regístrese, comuníquese, publíquese y archívese.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

CÉSAR VILLANUEVA ARÉVALO
Presidente del Consejo de Ministros

1740637-2

Anexo N° 08: Fragmento del convenio de Budapest

Artículo 6 – Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

- a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
 - i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;
 - ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

- b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

https://www.oas.org/juridico/english/cyb_pry_convenio.pdf