UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO,2020 -2022.

Tesis para optar el título profesional de

ABOGADO

KATY ARACELI SALCEDO PIÑA

JESÚS FELIPE GRANADOS PAREDES

Pucallpa - Perú

2026

ACTA DE EXAMEN PARA OPTAR EL TITULO DE ABOGADO

En la ciudad de Pucallpa, siendo las 5:00 pm del día miércoles 15 de enero del año 2026, en el auditorio de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de Ucayali, cito en el Tercer Piso de la Facultad de Derecho y Ciencias Políticas, se dio inicio a la correspondiente sustentación y/o defensa de la tesis denominada "DESARROLLO DE LOS DELITOS INFORMATICOS EN EL SISTEMA PENAL PERUANO 2020-2022", presentado por los bachilleres en Derecho y Ciencias Políticas: **KATY ARACELI SALCEDO PIÑA Y JESUS FELIPE GRANADOS PAREDES.**

En cumplimiento del Reglamento de Grados y Títulos, el Secretario Académico de la Facultad procedió a presentar a los Miembros del Jurado integrados por los docentes: Dr. JUAN ARQUIMEDES NUÑEZ TERREROS (Presidente), Dr. ELADIO GUZMAN VILLA (Miembro) y Soc. WASHINGTON T. QUINTANILLA OSORIO (Miembro), designados con Memorando Múltiple Nº 001-2026-UNU/FDyCP/GyT de fecha 13 de enero 2026; luego del cual el señor presidente instó al Secretario Académico a presentar a los bachilleres examinados.

Acto seguido el Presidente del Jurado invitó a los bachilleres a iniciar la exposición, del informe final de tesis; a cuyo término los miembros del jurado formularon las preguntas y objeciones respectivas, la misma que fueron absueltas de forma parcialmente satisfactoria por los ponentes.

Continuando con el desarrollo de la sustentación y de conformidad con el Reglamento de Grados y Títulos, el presidente invitó a los bachilleres examinados y al público asistente a abandonar la Sala para su correspondiente deliberación en forma reservada.

Seguidamente el Jurado emitió la calificación general, de cuyo resultado se establece que los bachilleres: **KATY ARACELI SALCEDO PIÑA Y JESUS FELIPE GRANADOS PAREDES** fueron APROBADOS POR MAYORIA.

Reiniciando el acto Público se procede a la Juramentación de honor y las felicitaciones por los miembros del Jurado, procediéndose a la lectura de la presente acta, dando por concluido el acto de sustentación siendo la 6:00 pm. Del mismo día, lo suscribieron en señal de conformidad; de lo que doy fe.

Dr. JUAN ARQUIMEDES NUÑEZ TERREROS
PRESIDENTE

Dr. ELADIO GUZMAN VILLA
MIEMBRO

Soc. WASHINGTON T. QUINTANILLA OSORIO
MIEMBRO

Dr. RUBEN ADOLFO CERNA LEVEAU
SECRETARIO ACADÉMICO (e)

ACTA DE APROBACIÓN

La presente tesis fue aprobada por los miembros del Jurado Evaluador de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de Ucayali como requisito para optar el Título Profesional de Abogado.

Dr. Juan Arquímedes Núñez Terreros

Presidente

Dr. Eladio Guzmán Villa

Miembro

Soc. Washington Tarsicio Quintanilla Osorio

Miembro

Dr. Joel Orlando Santillan Tuesta

Asesor

Bach. Katy Araceli Salcedo Piña

Tesista

Bach. Jesús Felipe Granados Paredes

Tesista

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº V/376-2025.

La Dirección de Producción Intelectual de la Universidad Nacional de Ucayali, hace constar por la presente, que el trabajo académico de investigación, titulado:

"**DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO,2020 -2022**"

Autor(es)	:	**SALCEDO PIÑA, KATY ARACELI**
		GRANADOS PAREDES, JESÚS FELIPE
Facultad	:	**DERECHO Y CIENCIAS POLÍTICAS**
Escuela	:	**DERECHO**
Asesor(a)	:	**Dr. SANTILLAN TUESTA, JOEL ORLANDO**

Presenta un **porcentaje de similitud de 9%,** verificado en el Sistema Antiplagio COMPILATIO,

De acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO, el cual indica que todo trabajo de investigación no debe superar el 10%. **En tal sentido, se declara, que el presente trabajo de investigación: SI Contiene un porcentaje aceptable de similitud,** procediéndose a emitir la presente Constancia de Originalidad de Trabajo de Investigación (COTI) a solicitud del asesor.

En señal de conformidad se firma y sella el presente documento.

Fecha: 30/07/2025

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, KATY ARACELI SALCEDO PIÑA

Autor de la tesis titulada : " DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO 2020-2022".

Sustentada el año 2026

Asesor(a): Dr. JOEL ORLANDO SANTILLAN TUESTA

Facultad: DERECHO Y CS. POLÍTICAS

Escuela Profesional: DERECHO

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 15/01/2026

Email: Katyaraceli salcedopina@gmail.com Firma:

Teléfono: 978066296 DNI: 62406955

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, JESUS FELIPE GRANADOS PAREDES

Autor de la tesis titulada: " DESARROLLO DE LOS DELITOS INFORMATICOS EN EL SISTEMA PENAL PERUANO 2020-2022".

Sustentada el año: 2026

Asesor(a): Dr. JOEL ORLANDO SANTILLAN TUESTA

Facultad: DERECHO Y CS. POLITICAS

Escuela Profesional: DERECHO

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 15/01/2026

Email: ducke.2022@gmail.com Firma:

Teléfono: 925521315 DNI: 71053082

DEDICATORÍA

Esta tesis es un testimonio de mi crecimiento personal y profesional, impulsado por tu presencia en mi vida. Gracias por darme la oportunidad de ser esa persona adulta que quise para mí y hoy puedo ser con todo mi amor y gratitud para ti Nury Rodas Piña. Tu hermana mayor.

Katy Salcedo

Dedico esta tesis a mis padres, el motor que impulsó cada esfuerzo y sacrificio en esta travesía académica, cuya sabiduría y amor inquebrantable me guiaron en cada paso.

Jesús Granados

AGRADECIMIENTOS

Quisiera comenzar expresando mi más sincero agradecimiento a mi tutor de tesis, el Dr. Joel Orlando Santillán Tuesta, cuya experiencia, paciencia y apoyo constante fueron fundamentales para la realización de este trabajo. Su guía no solo me proporcionó claridad académica, sino también motivación en momentos de duda. Su confianza en mí me impulsó a seguir adelante y superar los desafíos.

Katy Salcedo

A mi familia, especialmente a mis padres, les agradezco profundamente su amor incondicional y su apoyo constante. Su fe en mí ha sido el motor que me permitió completar este camino. A mis hermanos, por sus palabras de aliento, y a mis abuelos, por su presencia y cariño, gracias por ser mi pilar en los momentos difíciles. Sin ustedes, este logro no habría sido posible.

Jesús Granados

ÍNDICE GENERAL

DEDICATORÍA vii

AGRADECIMIENTOS viii

ÍNDICE GENERAL ix

ÍNDICE DE TABLAS xi

ÍNDICE DE FIGURAS xii

RESUMEN xiii

ABSTRACT xiv

INTRODUCCIÓN xv

CAPÍTULO I: EL PROBLEMA DE LA INVESTIGACIÓN 1

1.1. Descripción del Problema 1

1.2. Formulación del Problema 3

1.2.1. Problema general 3

1.2.2. Problemas específicos 4

1.3. Formulación de objetivos 4

1.3.1. Objetivo general 4

1.3.2. Objetivos específicos 4

1.4. Justificación de la investigación 4

1.5. Delimitación de estudio 6

1.6. Viabilidad del Estudio 6

CAPÍTULO II: MARCO TEÓRICO 8

2.1. Antecedentes jurídicos del problema 8

2.1.1. Antecedentes internacionales 8

2.1.2. Antecedentes nacionales 8

2.1.3. Antecedentes locales 9

2.2. Bases teóricas 10

2.3. Definición de términos básicos 26

2.4. Formulación de hipótesis 27

2.4.1. Hipótesis general 27
2.4.2. Hipótesis específicas 27
2.4. Variables 27
CAPÍTULO III: METODOLOGÍA 30
3.1. Diseño de la Investigación 30
3.2. Población y muestra 31
3.3. Técnicas e Instrumentos de Recolección de Datos 31
3.4. Validez y Confiabilidad del Instrumento 31
3.5. Técnicas para el Procesamiento de la Información 32
CAPÍTULO IV: RESULTADOS Y DISCUSIONES 33
4.1. Descripción de resultados 33
4.2. Discusión de resultados 53
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 59
5.1. Conclusiones 59
5.2. Recomendaciones 60
REFERENCIAS BIBLIOGRÁFICAS 61
ANEXOS 64

ÍNDICE DE TABLAS

Tabla 1. El verbo rector……22

Tabla 2. El ciberdelincuente ataca……..25

Tabla 3. Operacionalización de las variables……29

Tabla 4. Entrevista número Uno – realizado a los Fiscales 33

Tabla 5. Resultados de Entrevista número Uno – realizado a los Fiscales.....34

Tabla 6. Entrevista número Dos – realizado a los Fiscales 35

Tabla 7. Resultados de Entrevista número Dos – realizado a los Fiscales.....36

Tabla 8. Entrevista número Tres – realizado a los Fiscales.....37

Tabla 9. Resultados de Entrevista número Tres – realizado a los Fiscales 38

Tabla 10. Entrevista número Cuatro – realizado a los Fiscales 39

Tabla 11. Resultados de Entrevista número Cuatro – realizado a los Fiscales 40

Tabla 12. Entrevista número Cinco – realizado a los Fiscales.....41

Tabla 13. Resultados de Entrevista número Cinco – realizado a los Fiscales 42

Tabla 14. Entrevista número Seis – realizado a los Fiscales.....43

Tabla 15. Resultados de Entrevista número Seis – realizado a los Fiscales 44

Tabla 16. Entrevista número Siete – realizado a los Fiscales …….....45

Tabla 17. Resultados de Entrevista número Siete – realizado a los Fiscales..... 46

Tabla 18. Entrevista número Ocho – realizado a los Fiscales 47

Tabla 19. Resultados de Entrevista número Ocho – realizado a los Fiscales.....47

Tabla 20. Entrevista número Nueve – realizado a los Fiscales 48

Tabla 21. Resultados de Entrevista número Nueve – realizado a los Fiscales..... ...49

Tabla 22. Entrevista número Diez – realizado a los Fiscales.....50

Tabla 23. Resultados de Entrevista número Diez – realizado a los Fiscales..... 50

Tabla 24. Entrevista número Once – realizado a los Fiscales 52

Tabla 25. Resultados de Entrevista número Once – realizado a los Fiscales.....52

ÍNDICE DE FIGURAS

Figura 1. Resultados de Entrevista número Uno – realizado a los Fiscales 34

Figura 2. Resultados de Entrevista número Dos – realizado a los Fiscales 36

Figura 3. Resultados de Entrevista número Tres – realizado a los Fiscales 38

Figura 4. Resultados de Entrevista número Cuatro – realizado a los Fiscales.....40

Figura 5. Resultados de Entrevista número Cinco – realizado a los Fiscales 42

Figura 6. Resultados de Entrevista número Seis – realizado a los Fiscales.....44

Figura 7. Resultados de Entrevista número Siete – realizado a los Fiscales 46

Figura 8. Resultados de Entrevista número Ocho – realizado a los Fiscales.....48

Figura 9. Resultados de Entrevista número Nueve – realizado a los Fiscales 49

Figura 10. Resultados de Entrevista número Diez – realizado a los Fiscales 51

Figura 11. Resultados de Entrevista número Once – realizado a los Fiscales ……..53

RESUMEN

El presente trabajo de investigación tuvo como objetivo general determinar el desarrollo de los delitos informáticos en el sistema penal peruano tipificados en la Ley Especial Nº 30096 modificado por Ley Nº 30171 en los años, 2020 - 2022; su diseño de investigación que se trabajó fue el método inductivo y deductivo; se utilizó el tipo de investigación básica o teórica, que se caracteriza por ser naturalista, fenomenológica, interpretativo. El nivel de investigación que se utilizó fue descriptivo, porque se describió el fenómeno de los delitos informáticos que se desarrolla en el sistema penal peruano, así mismo; el estudio fue de diseño no experimental; con una población muestra de cinco fiscalías provinciales penales corporativas de coronel portillo, que están integrados de cuatro despachos cada uno, un titular y tres adjuntos, que en total suman 20 integrantes, utilizando la técnica de la entrevista dado que esto nos permitió obtener información de manera directa y someter a un análisis por objetivos y como instrumento se utilizó el cuestionario; posteriormente nos manda a una conclusión en que se ha logrado determinar que el desarrollo de los delitos informáticos en el sistema penal peruano tipificados en la Ley Especial Nº 30096 modificado por Ley Nº 30171 en los años, se encuentra en continuo desarrollo a la par con los avances tecnológico continuo, cuyo indicador de este fenómeno jurídico es las modificaciones introducidas desde el año 2013 hasta la actualidad.

Palabras claves: Delitos, Informáticos, Sistemas, Tipificados.

ABSTRACT

The general objective of this research work was to determine the development of computer crimes in the Peruvian criminal system typified in Special Law No. 30096 modified by Law No. 30171 in the years, 2020 -2022; The research design used was the inductive and deductive method; The type of basic or theoretical research was used, which is characterized by being naturalistic, phenomenological, and interpretive. The level of research used was descriptive, because the phenomenon of computer crimes that develops in the Peruvian criminal system was described, as well; The study was non-experimental in design; with a sample population of five corporate criminal provincial prosecutor's offices of Colonel Portillo, which are made up of four offices each, one head and three deputies, which in total add up to 20 members, using the interview technique since this allowed us to obtain information from directly and subject to an analysis by objectives and the questionnaire was used as an instrument; subsequently leads us to a conclusion in which it has been determined that the development of computer crimes in the Peruvian criminal system typified in Special Law No. 30096 modified by Law No. 30171 over the years, is in continuous development along with the continuous technological advances, whose indicator of this legal phenomenon is the modifications introduced from 2013 to the present.

Keywords: Crimes, Computer Science, Systems, Typified.

INTRODUCCIÓN

En las últimas décadas, el desarrollo tecnológico en general e informático en particular es galopante, especialmente proveniente de China, Japón, Estados Unidos de Norteamérica, Rusia y otros países; cuyo uso es bifronte, por un lado es muy útil para el desarrollo de servicios y facilita a las actividades de transacción bancaria, así como personales domésticas, porque desde cualquier lugar deslizas dinero sin necesidad de estar presente o hacer colas inmensas y largas como se aprecia cada mes en el Banco de la Nación de Pucallpa; por otro lado, estas mismas conductas es usada por los ciberdelincuentes para hurtar o trasladar ilícitamente a otras cuentas a partir de una clave o contraseña jaqueado o copiado clandestinamente.

Sanchis (2024). En el sistema penal peruano, los delitos informáticos se encuentran regulados en el Código Penal; sin embargo, en el Perú también se desarrollan tanto como agravantes de algunos delitos tipificados en dicho cuerpo normativo como en una ley especial, según informa el Instituto Nacional de Ciberseguridad (INCIBE), el Ministerio del Interior, el Observatorio Español de Delitos Informáticos (OEDI) y la Europol, sostienen que “la ciberdelincuencia es una de las mayores amenazas sobre todo de las grandes empresas, pero ninguna queda excluida del “grupo de riesgo”, así como tampoco lo estamos el resto de los usuarios”. Con la finalidad de tratar de comprender el fenómeno de la ciberdelincuencia, se procede realizar el estudio, separando en capítulos, el primer capítulo se desarrolla el problema de investigación, en el segundo capítulo se desarrolla el marco teórico, en el tercer capítulo se plasma la metodología usada, en el cuarto capítulo se ha desarrollado los resultados obtenidos, seguidamente se llega a las conclusiones y recomendaciones.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

La informática o la computación en la actualidad a copado todas las actividades del ser humano, se ha convertido en una necesidad prioritaria y en una herramienta muy importante para desarrollar muchas actividades, debido a la capacidad de almacenar, procesar y tramitar información y datos en forma digital; sin embargo, también se ha convertido en una herramienta perfecta para ocultar al delincuente de sus víctimas mediante enlace digital.

Puelles (2021). El problema que salta a la vista, que consideramos los más importantes es primero la falta de tipificación como delitos informáticos, muchos hechos que afectan bienes jurídicos a las personas físicas y jurídicas; segundo el delito informático cada día va en aumento descontroladamente, oculto tras el enlace digital el sujeto activo va asechando a sus víctimas permanentemente y tercero la impunidad debido a que solamente 2% son procesados o encausados y el 97.87% no están encausados.

El delito que se comete usando la informática es variada y múltiple, de allí que, el Estado en todas partes, ha visto por conveniente implementar ciertas conductas mediante el uso digital que sean tipificados como delito, ante la inseguridad de la persona física y la persona jurídica mediante los delincuentes cibernéticos, son afectados mediante muchas modalidades, como compras, trasferencias, estafas, fraudes y otros.

Naciones Unidas – Departamento de Asuntos Económicos y Sociales (s. f.). Las Naciones Unidas, a traves del Departamento de Asuntos Económicos y Sociales, ya desde el año 2010 señalaban que “las amenazas en el ciberespacio han aumentado dramáticamente perjudicando a 431 millones de víctimas adultas

en todo el mundo, lo que equivale a catorce víctimas adultas por segundo y a un millón de víctimas de delitos cibernéticos por día a nivel mundial".

Ehrhart (2023). Se pronostica, según el "Barómetro de Riesgo de Alianza calcula, que en el año 2023 el costo promedio por robo de datos a empresas será superior a los 5 millones de dólares".

Sanchis (2024). En España, el Ministerio de Interior público un reporte Estadístico que refleja que, durante el primer semestre del año 2023, el 18,3% de los crímenes se cometieron por medios digitales, lo que representa un incremento del 19,7 % en comparación con el año anterior; ello indica que este fenómeno se encuentra en constante aumento.

Puelles (2021). En una evaluación realizada con una tasa de 100,000 habitantes en el Perú, se observa que, antes del año 2002, los delitos presentaban una tasa menor a 0,1, lo que permite calificarlos como muy bajos a nivel nacional. A partir del año 2007, esta tasa se incrementó de 0,1 a 1,8, ubicándose en un rango bajo. Desde el año 2012, el índice aumentó de 1,9 a 3,9, correspondiente a un rango medio, y alcanzó valores de entre 3,7 y 5,3, considerados como muy altos, especialmente en ciudades como Lima.

"La Policía Nacional del Perú (PNP) registró 14 671 denuncias por delitos informáticos en 2021, lo que representa un incremento del 65 % respecto de las 8 897 denuncias reportadas en 2020" (Perù, 2022); los datos indican el incremento paulatino de los delitos informáticos; hoy el delincuente no necesita conocerte, enfrentarte y arrebatarte de tus pertenencias, los ciber delincuentes desde muy lejos puede estar asechándote para arrebatar tus pertenencias mediante aplicativos informáticos.

Según el Boletín Estadístico del Ministerio Público de marzo 2019, citado por Puelles (2021) el primer problema identificado es que 9 619 casos no se encuentran tipificados ni subsumidos en alguna figura delictiva prevista en la Ley N.º 30096 y su modificatoria, lo que evidencia la existencia de numerosos hechos

que vulneran bienes jurídicos tutelados y que no son investigados; el segundo problema es el aumento constante del delito de fraude informático en nuestro país, el 2015 (49 casos), 2016 (189 casos), 2017 (778 casos), 2018 (1984 casos), 2019 (3039 casos) y 2020 (935 casos), en términos generales el fenómeno jurídico social del delito informático va en aumento en nuestro país, que durante el confinamiento por COVID-19 llegó a su pico más elevado; el tercer problema en el mismo periodo de los 6,474, se archivó 1925, se aplicó principio de oportunidad solamente 15 casos, se dictó reserva provisional 13 casos, se dictó imputación de cargo únicamente en 21 casos y se formalizo la investigación preparatoria en 117 caso, terminación anticipada 01 y sentencia 10 casos; es decir, únicamente 2.13% de casos está encausado y 97.87% no están encausados.

Según Vinelli (2021) en el año 2020:

> En Perú, entre abril y la primera semana de agosto de 2020, se registraron 1.481.963 ataques de pishing, con un promedio de 7.000 ataques por día. Por otro lado, de enero a julio de 2020, se recibieron 1117 denuncias de fraude informático. De estas, 974 se debieron a transacciones o transferencias electrónicas no autorizadas y 142 a fraudes cometidos en línea. (p.97).

En el ámbito regional los delitos informáticos también siguen en aumento, según Puelles (2021) antes del 2007 el delito informático estuvo menor a 0.1 en una población de 100, 000 habitantes y 2012 subió a 0.1 a 1.8 a un rango bajo, sin embargo, debemos señalar, conforme crece la población, el delito se va incrementando en Ucayali, especialmente en trata de personas, hurto mediante cajeros automáticos, suplantación de claves y otros.

1.2. Formulación del problema

1.2.1. Problema general

- ¿Cuál es el desarrollo de los delitos informáticos en el sistema penal peruano tipificados en la Ley especial Nº 30096 modificado por Ley Nº 30171 en los años, 2020 -2022?

1.2.2. Problemas específicos

- ¿Por qué los hechos que afectan bienes jurídicos a personas físicas no están tipificados como delitos informáticos en el sistema penal peruano?
- ¿Por qué los delitos informáticos registran el incrementan permanentemente en el sistema penal peruano, 2020-2022?
- ¿Cuáles son los factores de la impunidad en los delitos informáticos en el sistema penal peruano?

1.3. Formulación de objetivos

1.3.1. Objetivo general

- Determinar el desarrollo de los delitos informáticos en el sistema penal peruano tipificados en la Ley Especial Nº 30096 modificado por Ley Nº 30171 en los años, 2020 -2022.

1.3.2. Objetivos específicos

- Establecer los hechos que afectan bienes jurídicos a personas físicas no están tipificados como delitos informáticos en el sistema penal peruano.
- Establecer el incremento de los delitos informáticos en el sistema penal peruano. 2020 -2022.
- Establecer los factores de la impunidad en los delitos informáticos en el sistema penal peruano.

1.4. Justificación de la investigación

Justificación teórica*:* Desde el ámbito teórico el delito informático se encuentra en pleno desarrollo, que a la par con los avances tecnológicos, se va creando estereotipos complejos y especiales, porque el delincuente no es el tipo que presentó Lombroso, es decir es un sujeto con conocimientos especiales y habilidades del manejo de alta tecnología de saco y corbata, muy refinado y con estudios superiores; es un delincuente contemporáneo, por lo que se requiere de una atención especial y especializada del Estado para prevenir y sancionar este tipo de delitos; asimismo, se requiere eficiencia y eficacia en la obtención de

pruebas porque son volátiles, que se puede borrar y fácilmente desaparecer; por ello la tesis, tiene importancia porque ha contribuido teóricamente en la construcción de categorías, conceptos y definiciones; asimismo, sirvió como antecedente para continuar con otras investigaciones de los profesionales de derecho.

Justificación practica: El delito informático está aumentando en los últimos años, la falta de empleo y apoyo en las pequeñas y micro empresas, hacen que los jóvenes talentosos volcán sus conocimientos para conseguir dinero fácil, mediante la suplantación de identidad; asimismo, se motivó a los funcionarios del Estado, el personal que se encuentra en la pesquisa, investigación y sanción deben tener especiales habilidades en el manejo de la cibernética, con el fin de enfrentar en plano de igualdad o superar a los delincuentes, en la obtención y conservación de las pruebas, el almacenamiento y detección de las comunicaciones con autorización judicial.

Justificación metodológica: En el aspecto metodológico la tesis fue de enfoque cualitativo, donde se utilizó los métodos muy conocidos de análisis-síntesis, inductivo-deductivo, el método histórico, empleando la hermenéutica en la interpretación de normas jurídicas vigentes, sin dejar de lado la metodología planteada de la facultad de derecho y ciencias políticas.

Importancia: La tesis es muy importante, porque permitió conocer y profundizar categorías, sub categorías, conceptos y definiciones del delito cibernético, que navegando por las nubes puede captar a las cándidas víctimas, para suplantar su identidad, con la cual, retirar el dinero a diferentes cuentas, que superan de 15 o más cuentas son distribuidas, organizado por una organización camuflada.

Viabilidad: El proyecto es viable, porque fue auto financiada, con el fin de compartir gastos, nos hemos unidos dos estudiantes, según a lo permitido por el reglamento de la universidad hasta entonces; por otro lado, el tiempo de estudio

es razonables porque radicamos en la ciudad, lo que nos permitió recoger nuestros datos con mayor facilidad.

1.4. Delimitación del estudio

Delimitación espacial: El estudio se realizó, en las cinco fiscalías penales corporativas de Coronel Portillo-Ucayali, cada fiscalía cuenta, con un titular y tres adjuntos, que en total suman 20 fiscales.

Delimitación temporal: En la presente investigación se centró en el periodo de 12 meses correspondientes al año 2022.

Delimitación teórica: La investigación, describió todos los delitos informáticos y la suplantación de identidad de las víctimas.

1.5. Viabilidad del estudio

Viabilidad técnica: El estudio, desde el aspecto metodológico fue viable, debido a que siguió con el Reglamento de Grados y Títulos de la Universidad, en el marco de la Ley Universitaria.

Viabilidad ambiental: El estudio presenta un enfoque estrictamente teórico y de abstracción de la realidad, por lo que no implica la ejecución de actividades de campo ni la utilización de recursos naturales. En consecuencia, no existe la posibilidad de que, de forma directa o indirecta, se genere algún impacto negativo sobre el medio ambiente, encontrándose garantizada su viabilidad ambiental.

Viabilidad financiera: El estudio, fue auto financiado, porque los tesistas cubrieron íntegramente todo el costo del trabajo de investigación, procurando usar los medios tecnológicos, para revisar, libros, revistas, artículos, información y otros.

Viabilidad social: El estudio es de carácter académico y jurídico, y se desarrolla desde un enfoque objetivo e imparcial, sin orientación hacia creencias religiosas ni hacia posturas ideológicas o políticas que puedan generar controversia. En tal sentido, la investigación no afecta valores sociales ni intereses

colectivos, sino que busca contribuir al análisis y comprensión de una problemática jurídica de relevancia social, por lo que se encuentra plenamente garantizada su viabilidad social.

CAPÍTULO II

MARCO TEÓRICO REFERENCIAL

2.1. Antecedentes jurídicos del problema

2.1.1. Antecedentes internacionales

Según Fonseca & Martinez (2022); en su investigación titulado “Los delitos informáticos y la problemática trasnacional: el caso colombiano”, El objetivo es determinar las protecciones legales y regulatorias que el gobierno colombiano ha ofrecido contra los delitos relacionados con la información, Este capítulo, que se basa en una investigación cualitativa, examina los orígenes del cibercrimen y la transformación que se produce en el intercambio de información en la actualidad debido a que el fenómeno no se limita a un solo país, requiriendo que sus características tengan una conexión transnacional.

En consecuencia, el manejo que brindan los sistemas jurídicos internacionales y latinoamericanos al sistema de justicia penal que transmite los medios de comunicación tridimensionales requiere especial atención a los derechos de los sujetos involucrados y una conciliación efectiva del tratamiento informativo, necesitando herramientas como la cooperación internacional que posibiliten una respuesta priorizada y contundente a los habitantes del territorio nacional.

2.1.2. Antecedentes nacionales

Según Peralta (2022) en su tesis titulada “Los delitos informáticos y los datos en sistema informático”, en una investigación, teórica, descriptiva, llego a las siguientes conclusiones:

A medida que el mundo se ha globalizado, la modernidad ha propiciado el uso del almacenamiento de datos personales a escala global así como en diversas entidades públicas y privadas, bajo el respaldo de

medidas de seguridad esenciales como garantías para sus operaciones, lo que no supone un problema para ciertas organizaciones criminales o los llamados cibercriminales quienes, utilizando técnicas o procedimientos tecnológicos sofisticados, acceden a las cuentas bancarias de sus potenciales víctimas, vaciando sus cuentas bancarias o apoyando actividades comerciales.

Estos ciberataques tienen como objetivo dañar los sistemas de información de las víctimas y causar perjuicios materiales, mediante la obtención indebida y el uso fraudulento de sus datos, estas acciones afectan la seguridad digital.

El objetivo de estos ciberataques no siempre es atacar directamente las fuentes de financiación de las empresas; también pueden tener como objetivo robar, ocultar o alterar información privada.

Los casos de Ciberataques Señalados demuestran cómo este tipo de delito puede tener un impacto significativo en los sistemas digitales y de información. En Perú, los ciberataques se originan en países distantes como Rusia y Moldavia, y se dirigen a grandes corporaciones, bancos y ciudadanos particulares. Los sistemas de información de diversas agencias estatales han sido objeto de ciberataques, poniendo a disposición del público todos los datos que protegían. Esto demuestra la enorme vulnerabilidad de la información digital en nuestro país.

2.1.3. Antecedentes locales

Como indica Cataño & Panduro (2023); en su Investigación titulada “El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo - Ucayali 2022”, y se planteó como objetivo de estudio, determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022, es un estudio cuantitativo con diseño no experimental y nivel

correlacional. Se planteó la siguiente pregunta general de investigación: ¿Cómo se produce el robo de información en las operaciones financieras de los bancos de la provincia de Coronel Portillo?, basándonos en la siguiente hipótesis general de investigación, el robo de información de los bancos de la provincia de Coronel Portillo se produce de forma significativa en las operaciones financieras, y sus variables de estudio incluyen operaciones financieras y robo de información, que incluyen aspectos de investigación sobre acceso a base de datos, uso ilegal de información, phishing, gestión de riesgos y otorgamiento de créditos; Se utilizaron 263 personas de entre 18 y 70 años con cuentas bancarias como participantes del estudio. Se les formularon preguntas y se recabó su opinión sobre el tema investigado. También se utilizaron estadísticas descriptivas con un nivel de confianza del 95 % y un coeficiente de correlación de 0,756, lo que demuestra una fuerte correlación positiva entre las variables del estudio.

2.2. Bases teóricas

2.2.1. Base epistemológica, definiciones etimológicas, parte histórica

- **Epistemología**

El estudio, teóricamente se sustenta en el positivismo jurídico, especialmente el enfoque de Hans Kelsen, debido a que el fenómeno del estudio es real, tanto en el plano social y en el plano jurídico, adquiriendo su validez científica, como lo señala Ramos (2008), que la “epistemología es sinónimo de validez del conocimiento, así como gnoseología.” (p.15).

En la sanción del delito se desarrolla en el marco del principio de legalidad, conforme lo establece el Código Penal del Perú, en su Art. II del Título Preliminar “Nadie será castigado por un hecho que no esté tipificado como delito o falta por la ley vigente al tiempo de su comisión, ni estará sujeto a penas o medidas de seguridad que no estén señaladas en ella; en consecuencia, el círculo se completa con el artículo siguiente, que señala

que "no es posible utilizar la analogía para determinar si el hecho fue delito o falta" (art.III,TP- CP), lo que significa, ninguna autoridad puede crear o inventar un delito, ni penas ni medidas de seguridad, solamente la ley.

- **Definiciones etimológicas**

El delito, es una palabra que etimológicamente nace del término latín *delictum*, que significa falta, error o descuido, Arnal (s.f.); en cambio, la palabra suplantación surge de la palabra *supplantear* que significa falsificar, derribar o zancadillar (RAE), seguidamente la palabra identidad "surge del latín *identitas* que expresa la calidad de algo idéntico, mismidad y continuidad. Albuqueroque (s.f.). Se puede decir que su uso se vincula a la lógica y a las matemáticas como una relación abstracta de elementos iguales".

- **Historia**

La palabra informático, fue acuñado el año 1962, por el ingeniero francés Philleppe Dreyfus, quien a su vez lo tomó de Karl Steinbuch, científico alemán, que en el año 1956 publicó un trabajo científico, al cual tituló Informática: procesamiento automático de información.

Según explica el Centro de Estadistica de Observatorio y Monitoreo de ciberdelitos - OGDI (s.f.), los delitos iniciaron de manera paulatina, conforme iba avanzando la comunicación y la informática, así tenemos:

En la década de 1970, los delincuentes cometían ilícitos a través de líneas telefónicas y eran denominados phreakers. Estos descubrieron que los teléfonos funcionaban con base en tonos, los cuales imitaban para realizar llamadas gratuitas, constituyendo así una forma rudimentaria de cibercrimen.

En la década de 1980 se comenzaron a hackear computadoras para copiar o manipular datos e información personal. En 1981, Ian Murphy, conocido como Capitán Zap, fue declarado culpable por primera

vez de un delito cibernético, tras piratear una compañía telefónica en Estados Unidos y manipular su reloj interno, permitiendo llamadas gratuitas en horas pico. En ese contexto, los primeros objetivos del cibercrimen fueron principalmente las empresas telefónicas, los bancos, las tiendas y las personas.

En los años siguientes, se han producido numerosos delitos cibernéticos, caracterizados por fraudes millonarios que se vienen incrementando progresivamente, teniendo como principales objetivos a las personas, las empresas y los bancos, de los cuales se obtiene una gran cantidad de dinero.

Este fenómeno motivó a los organismos internacionales a suscribir convenios multilaterales con la finalidad de prevenir y sancionar los delitos cibernéticos. Entre ellos destacan: a) el Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001; y b) el Convenio Iberoamericano de Cooperación sobre Investigación, Garantía y Obtención de Pruebas en Materia de Ciberdelincuencia, mediante los cuales se busca mejorar las técnicas de investigación, la prevención del delito y la cooperación entre los Estados.

Defensoria del Pueblo (2023). En Perú, el Código Penal, publicado el 8 de abril de 1991, definió inicialmente el daño telemático como un delito que "consiste en la utilización de sistemas de transferencias electrónicas de fondos o telemáticos en general, o en la violación del uso de claves secretas, para respaldar total o parcialmente bienes ajenos y, de esta forma, apoderárselos ilegítimamente".

Defensoria del Pueblo (2023). Luego de nueve años, el 17 de julio de 2000 se publicó la ley Nº 27309, que agregó a la lista de delitos el apartado sobre delitos contra el patrimonio del código penal, conocidos como "delitos informáticos". Originalmente, “incluían el delito de robo de

información propiamente dicho (artículo 207-A); la alteración, destrucción de bases de datos, sistemas informáticos, redes o programas (artículo 207-B); y sus formas agravadas (artículo 207-C)".

Defensoria del Pueblo (2023). Con la publicación de la Ley N° 30076 el 19 de agosto de 2013, se agregó a este capítulo el delito de tráfico ilícito de datos (artículo 207-D). Posteriormente, el 22 de octubre del año 2013, se publicó la Ley N.º 30096, Ley de Delitos Informativos. Finalmente, el 10 de marzo de 2014, se promulgó la Ley de Delitos Informativos, la cual fue modificada significativamente por la Ley N.º 30171.

2.2.2. Marco conceptual

- **Desarrollo del delito informático en el sistema penal peruano**

✓ **Concepto**

El delito informático, es muy complejo y pluriofensivo, por ellos, desde la teoría se ha venido construyendo una definición o abstracción que permite subsumir los distintos elementos del delito cibernético. Como lo señala Santiago Acurio del Pino, citado por Peralta (2022); en todas las actividades humanas existen "todo tipo de engaños, manipulaciones, codicia, fraude, venganza, etc.". Con el auge de la comunicación cibernética, surge nuevas formas de fraude, de robo, de espionaje, de sabotaje e incluso, acosos sexuales, trata de personas e incluso asesinatos, que afectan los bienes jurídicos y derechos fundamentales.

Subsumiendo los elementos de los delitos comunes, el delito informático es una acción humana, típica, antijurídica y culpable, cometido por medios electrónicos o cibernéticos contra una persona física o una persona jurídica, ocasionando daños y perjuicios.

Para Villavicencio Terreros (2014), citado por Vinelli (2021) "[…] Se trata de aquellas acciones destinadas a comprometer dispositivos de seguridad, como pueden ser sistemas informáticos, de correo o de datos

siendo vulnerados a través de una contraseña, son acciones típicas que sólo pueden llevarse a cabo a través de la tecnología" (p.98).

Según Rayón Ballesteros y Gómez Hernández (2014), citado por Vinelli (2021), el delito informático es Cualquier delito que involucre un dispositivo electrónico o internet, una computadora, un teléfono, un televisor, una grabadora de audio o video o un dispositivo electrónico en general puede ser utilizado para cometer el delito o puede ser objeto del mismo" (p.98).

✓ **Bien jurídico protegido**

Villavicencio (2014). Existe unanimidad en considerar que los delitos informáticos son delitos de carácter pluriofensivos, siendo el bien jurídico principal "la información almacenada, procesada y transmitida a través de los sistemas informáticos". (p. 288)

Para Peña (2008) el jurídico protegido es "la seguridad de los datos almacenados en bases de datos, redes o sistemas informáticos; o la seguridad del tráfico legal de datos que pasa a través de sus sistemas internos" (p. 501).

- **El delito informático en los tratados internacionales**

✓ **Convenio sobre la ciberdelincuencia- Budapest.**

El 23 de noviembre del 2001 se firmó el Convenio sobre la Ciberdelincuencia en Budapest, celebrado por el Consejo de Europa con asistencia de países miembros y no miembros. Luego de 18 años, mediante el Decreto Supremo N.º 010-2019-RE, del 10 de marzo del 2019, el Estado peruano ratificó el referido Convenio, publicando en el Diario Oficial El Peruano, el 22 de setiembre del 2019, vigente desde 1 de diciembre de dicho año.

El Convenio establece, en su preámbulo, la intensificación de la cooperación entre los Estados y la aplicación de una política común, con

el objeto de proteger a la sociedad frente a la ciberdelincuencia mediante una legislación adecuada y la promoción de la cooperación internacional; asimismo, garantiza el respeto de los derechos humanos y de otros tratados internacionales.

El Convenio se encuentra dividido en tres capítulos, el primer capítulo trata sobre la terminología; el segundo capítulo trata sobre las medidas que debe adoptarse a nivel nacional, y el tercero capítulo trata sobre la cooperación internacional:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informático.

a) Acceso ilícito.
b) Interceptación ilícita.
c) Ataque a la integridad de los datos.
d) Ataque a la integridad del sistema.
e) Abuso de los dispositivos.

- **Delitos informáticos**

a) Falsificación informática.
b) Fraude informático.

- **Delitos relacionados con el contenido**

a) Delitos relacionados con la pornografía infantil.

- **Delitos asociados a violaciones a la propiedad intelectual y al derecho al debido proceso**

a) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

- **Otras formas de responsabilidad y de sanción**

a) Tentativa y complicidad.
b) Responsabilidad con las personas jurídicas.
c) Sanciones y medidas.

- **Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Pruebas en materia de Delitos Cibernéticos**

✓ **El objetivo**

Los Ministros de Justicia Iberoamericanos (COMJIB) tienen por objeto reforzar la cooperación mutua entre las Partes para la adopción de medidas de aseguramiento y obtención de pruebas en la lucha contra la ciberdelincuencia, Esta cooperación investiga y persigue los delitos cibernéticos, garantizando la eficacia de los procedimientos penales y el respeto de los derechos.

✓ **Delito informático como un delito ordinario**

En el Código Penal de 1991, en su artículo 186 incluía como agravante del delito de hurto, el denominado hurto telemático, el cual fue derogado por la Única Disposición Complementaria Derogatoria de la Ley N.º 30096, publicada el 22 de octubre de 2013. Esta disposición buscaba reprimir formas de apropiación patrimonial cometidas mediante sistemas informáticos y mecanismos de transmisión electrónica, cuya norma establecía: “Mediante la utilización de sistema de trasferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas” (Inc.3, art.186).

“Utilizando el espectro radioeléctrico para la trasmisión de señales de telecomunicación ilegales” (Inc.6, art.186, CP).

Ley Nº 27309, publicada el 17 de julio del 2000, creó los delitos informáticos e incorporó los artículos 207-A, 207-B y 207-C al Código Penal:

Artículo 207.º-A.- El que utilice o ingrese a un sistema de cómputo, a una base de datos o a parte de estos sin autorización, para diseñar, ejecutar o alterar un esquema o similar, o que interfiera, intercepte, acceda

o copie datos en tránsito o contenidos en una base de datos, será sancionado con pena privativa de libertad de hasta dos años o con prestación de servicios a la comunidad de cincuenta a ciento cuatro jornadas.

Congreso de la Republica (2000). En el caso de que el agente actúe con la finalidad de obtener un beneficio económico, será sancionado con pena privativa de libertad no menor de tres años o con la prestación de servicios comunitarios por un período no menor de seis meses.

Artículo 207.º-B.- Cualquier persona que utilice, ingrese o interfiera indebidamente en una base de datos, sistema, programa de computadora o en cualquier parte de estos, con la intención de modificarlos, dañarlos o destruirlos, estará sujeta a una pena privativa de libertad no menor de tres ni mayor de treinta años.

Artículo 207.º-C.- En los casos previstos en los artículos 207.º-A y 207.º-B, la pena será privativa de libertad, no menor de cincuenta ni mayor de setenta años, si:

a) El agente accede a una información confidencial obtenida en el ejercicio de sus funciones para acceder a base datos, sistema o red informática.
b) El agente es responsable de la seguridad nacional, en tanto su conducta puede afectar intereses fundamentales del Estado, el orden público y la estabilidad institucional.

La Ley Nº 28251, publicada el 26 de mayo del 2002, incorpora en el artículo 183 el delito de turismo sexual infantil mediante el artículo 181.º-A y, en el artículo 183.º-A, el delito de pornografía infantil, cuya norma establecía:

- ✓ **Turismo sexual infantil**

Todo aquel que promueva, anuncie, fomente o facilite el turismo sexual, a través de cualquier medio escrito, sonoro, fotográfico, visual,

auditivo, electrónico, magnético o basado en Internet, con el fin de proporcionar relaciones sexuales comerciales entre hombres y mujeres menores de veinticinco años, será castigado con una pena privativa de la libertad no menor de dos ni mayor de seis años.

El agente estará sujeto a una pena privativa de la libertad no menor de seis ni mayor de ocho años cuando la víctima sea menor de diez años. Además, se impondrá la pena de inhabilitación, de conformidad con el artículo 36, incisos 1, 2, 4 y 5, del Código Penal.

Congreso de La Republica (2004). Si el hecho hubiera sido realizado por una autoridad pública, sus superiores, un maestro o quien hubiera tenido a su cargo el cuidado de la víctima a cualquier título, la pena será privativa de la libertad no menor de ocho ni mayor de diez años.

- ✓ **Pornografía infantil**

Congreso de La Republica (2004). Todo aquello que sea producido, promovido, fabricado, distribuido, exhibido, ofrecido, comercializado o hecho público a través de cualquier medio, incluido Internet, así como los objetos, libros, escritos, imágenes visuales o auditivas, o espectáculos en vivo de carácter pornográfico, que sean utilizados por personas entre las edades de cuatro y cinco años, será castigado con una pena mínima de seis años y máxima de cinco días de privación de la libertad.

No será menor de seis ni mayor de ocho años, y con setenta y cinco a treinta días-multa, si el menor tiene menos de catorce años. La pena privativa de la libertad no será menor de ocho ni mayor de diez años si la víctima se encuentra en alguna de las condiciones enumeradas en el último párrafo del artículo 173, o si el agente actuaba en calidad de empleado de una organización dedicada a la pornografía infantil. Una vez resuelto el caso, el agente quedará inhabilitado de conformidad con el artículo 36, incisos 1, 2, 4 y 5.

La Ley Nº 28774, publicada el 07 de julio del 2006, incorpora el Artículo 222.º-A, del Código Penal, la Clonación o Adulteración de terminales de telefonía celular, indica:

Artículo 222.º-A.- Será sancionado con pena privativa de libertad no menor de dos ni mayor de cinco años, y con sesenta a trescientos sesenta y cinco días-multa, quien altere, sustituya, duplique o modifique cualquier número de líneas o series electrónicas de manera que pueda causar perjuicio al titular o usuario de las mismas, así como a terceros.

El Decreto Legislativo Nº 982, publicada el 22 de julio del 2007, modifica el Artículo 316, del Código Penal, referente al delito de Apología al terrorismo, la cual señala:

La pena privativa de libertad no será inferior a seis ni superior a diez años si el delito se dirige contra actos de terrorismo o contra la persona que resulte ser su autor o partícipe. La pena no será inferior a ocho ni superior a quince años si se comete a través de medios sociales o mediante el uso de tecnologías de la información y la comunicación, como Internet u otros análogos, imponiéndose además trescientos sesenta días-multa e inhabilitación conforme a los incisos 2, 4 y 8 del artículo 36 del Código Penal (inc. 2, art. 316, CP).

La Ley Nº 29263, publicada el 20 de octubre del 2008, incorporó en el Artículo 220.º- A, 220.º-B, y 220.º-C, al Código Penal señala:

Artículo 220.º-A.- Será sancionado con pena privativa de libertad no menor de dos ni mayor de diez años quien, con ánimo de lucro u otro beneficio económico, eluda cualquier medida tecnológica utilizada por los fabricantes, intérpretes o ejecutantes de fonogramas, o por los autores de cualquier obra protegida por derechos de propiedad intelectual.

Artículo 220.º-B.- Productos destinados a la elusión de medidas tecnológicas. Quien fabrique, importe, distribuya, ofrezca al público,

suministre o comercialice de cualquier otro modo dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica utilizada por los fabricantes, intérpretes o ejecutores de fonogramas, así como por los autores de cualquier obra protegida por derechos de propiedad intelectual, será sancionado con pena privativa de libertad no menor de dos ni mayor de diez años.

Artículo 220º-C.- Congreso de la República (2008). Servicios destinados a la elusión de medidas tecnológicas. La persona que, con fines comerciales u otro tipo de beneficio económico, preste u ofrezca servicios al público principalmente para eludir una medida tecnológica utilizada por los fabricantes de fonogramas, intérpretes, ejecutores o autores de cualquier obra protegida por derechos de propiedad intelectual, será sancionada con pena privativa de libertad no menor de dos ni mayor de diez años.

El 22 de mayo del 2012, el Artículo 368.º- A y 368.º- B, del Código Penal, fueron incorporados por Ley N.º 29867, y modificado por Decreto Legislativo Nº 1182, publicado el 27 de julio del 2015, la cual señala:

Artículo 368.º-A: Todo aquel que ingrese ilegalmente, intente ingresar o facilite el ingreso a un centro de detención o aislamiento, incluyendo equipos o sistemas de comunicación, fotografía y/o filmación, o sus componentes que permitan la comunicación telefónica interna vía celular, línea fija, radio, Internet u otros medios análogos, así como el registro de fotografías, videos o la facilitación de claves de acceso a Internet desde el exterior del establecimiento penitenciario, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de seis años.

Artículo 368.º-B: Quien ilegalmente introduzca, intente introducir o permita la introducción de materiales o componentes susceptibles de ser

utilizados en la construcción de antenas, receptores u otros equipos que faciliten la comunicación telefónica interna por medios fijos, radiales, Internet u otros análogos, será sancionado con pena privativa de libertad no menor de dos ni mayor de cuatro años.

- **Delito informático como un delito especial**

En el sistema penal peruano, los delitos cibernéticos, originalmente regulados en el Código Penal de 1991, pasaron a una legislación especial. Ante el incremento paulatino de los ciberdelitos en el país y antes de la ratificación del Convenio de Budapest, el 22 de octubre de 2013 se promulgó la Ley N.º 30096 – Ley de Delitos Informáticos. Esta norma generó un pequeño debate en algunas universidades limeñas, al detectarse imprecisiones en la tipificación de las figuras delictivas, lo que dio lugar a una serie de proyectos de modificación en el Congreso y, finalmente, a la promulgación de la Ley N.º 30171, el 10 de marzo de 2014.

- **Los delitos según la Ley Especial Nº 30096 y su modificatoria Ley Nº 30171**

✓ **Modalidades del delito informático**

Delitos contra el sistema informático

1) Acceso ilícito

El acceso deliberado e ilegítimo a todo o parte de un sistema de información, siempre que se produzca sin que exista un fallo de seguridad que lo impida (…) el que accede a un sistema informático excediendo lo autorizado (art. 2, Ley Nº 30096).

2) Atentado a la integridad de datos informáticos

"Toda destrucción, introducción, deterioro, alteración, supresión o inaccesibilidad intencionada e ilícita de información será castigada con una pena de privación de libertad de un mínimo de tres años y un máximo de treinta y seis días." (art.3, Ley Nº 30096).

Tabla 1

El verbo rector

El sujeto que deliberadamente e ilegalmente	1. Daña 2. Introduce. 3. Borra. 4. Deteriora. 5. Altera 6. Suprime. 7. Hace inaccesible

3) Atentado a la integridad del sistema informático

El atentado contra la integridad del sistema informático se produce cuando el sujeto activo realiza “la subutilización intencional e ilegítima, total o parcial, de un sistema de información, impidiendo el acceso al mismo, dificultando o imposibilitando su funcionamiento o la prestación de sus servicios” (art. 4, Ley N.º 30096). La sanción prevista para este delito establece que “será castigado con pena privativa de libertad no menor de tres años y treinta y siete días”.

Hancco (2017). En general, se considera ciberseguridad de la información la protección de los dispositivos y sistemas de datos frente a conductas que buscan comprometer su seguridad, como el acceso no autorizado, la destrucción o el daño a bases de datos, programas y otros recursos informáticos. Estos delitos presentan características que solo pueden ser perpetrados mediante sistemas de información. (p. 30)

Asimismo, Hancco (2017) argumenta que la definición amplia de delito informático incluye todas las conductas en las que las TIC son utilizadas como medio para cometer ilícitos. La comisión de estos actos ilegales sugiere que las personas que los perpetran poseen especialización en su ejecución (p. 30).

- **Delitos informáticos contra la indemnidad y libertad sexual**

Sugerencias hechas a niños, niñas y adolescentes utilizando medios tecnológicos con fines sexuales.

- **Delito informático contra la intimidad y secreto de las comunicaciones**

✓ **Interceptación de datos informáticos**

Se considera sujeto activo aquel que "intercepta intencional e ilegítimamente información en transmisiones no públicas que se dirigen a un sistema de información, se originan en un sistema de información o se llevan a cabo dentro de uno, incluidas las emisiones electromagnéticas de un sistema de información que transmite la información" (art. 7, Ley N.º 30096).

- **Delitos informáticos contra el patrimonio**

✓ **Fraude informático**

Hancco (2017). Los sujetos buscan un beneficio patrimonial. La normativa regula cómo esta conducta implica alterar, borrar, suprimir, clonar o modificar un sistema de información hasta el punto de mantener a la víctima en un estado de error para ser explotada ilegalmente. Esto ocurre, por ejemplo, cuando se clonan sitios web de entidades financieras con el fin de obtener información financiera de las víctimas, apropiarse de sumas de dinero o realizar compras en su contra. (p. 30)

La Ley N.º 30096, en su artículo 8, establece que se considera sujeto activo a aquel que, de manera "intencional e ilegítima, busca dañar a otra persona o a sí mismo a través del diseño, introducción, alteración, borrado, supresión, clonación o cualquier interferencia o manipulación en el funcionamiento de un sistema de información".

- **Manipulación de datos de entrada**

Hancco (2017). Se caracteriza por el robo de códigos y claves que las víctimas utilizan para acceder a programas, almacenar datos u otros recursos. También ocurre cuando la víctima ingresa a programas o sitios web específicamente configurados para robar o manipular información. Por

ejemplo, esto puede suceder al clonar el sitio web de una institución financiera con el fin de obtener información de tarjetas de crédito. Además, estos delitos afectan directamente la seguridad y confianza en los sistemas informáticos, generando pérdidas económicas y vulnerando la privacidad de las personas. (p. 32)

- **Manipulación de datos de salida**

Hancco (2017) señala que este delito se relaciona con la información o datos que la víctima obtiene de un sistema de información. La utilización de información falsa permite a los delincuentes aprovechar el error de la víctima y la expone a consecuencias que benefician ilícitamente a los infractores (p. 32).

- **Manipulación de programas**

Hancco (2017). Este tipo de delito implica que los delincuentes intenten que los programas informativos de la víctima realicen actividades que el agente del delincuente ha ordenado para obtener un beneficio específico; esto requerirá cambiar el modo en que funcionan los programas informativos para lograr algún tipo de beneficio. (p. 33)

Hancco (2017). “Un método es el uso de troyanos, que son programas que ingresan bajo una solicitud de un software, pero comienzan a ejecutar el programa oculto en el sistema de la víctima que, por lo general, tiene como objetivo controlar de forma remota el ordenador de la víctima”. (p. 30)

- **Delitos informáticos contra la fe pública**

✓ **Suplantación de identidad**

Se considera suplantación de identidad cuando “las tecnologías de la información y la comunicación menoscaban la identidad natural o jurídica de una persona, siempre que dicha conducta genere cualquier tipo de daño material o moral”. Quien cometa este delito será sancionado con pena

privativa de libertad no menor de tres ni mayor de cinco años (art. 9, Ley N.º 30096).

- **Características de los delitos informáticos**

De acuerdo con Blossiers (2018), las principales características de los delitos informáticos son las siguientes:

- Conductas criminales de cuello blanco.
- acciones ocupacionales.
- acciones de oportunidad.
- provocan pérdidas económicas.
- muchos casos y pocas denuncias.
- Proliferación continua.
- Ilícitos de impunidad ante la ley.
- Delitos que genera robos por medio de tarjeta de crédito.
- Sistemas impersonales.
- Blossiers (2018). Fraudes que son deficientes de equiparar (p.28).

- **Suplantación de identidad**

✓ **Operaciones phishing (D1)**

Belcic (2020). “El phishing es una de las estafas en línea más antiguas y conocidas. Se puede definir como un tipo de fraude de telecomunicaciones que utiliza técnicas de ingeniería social para obtener información privada de las víctimas”.

Tabla 2

El ciberdelincuente ataca

Su ataque se dirige:	-Comunicación electrónica. -Correo electrónico. -Llamada telefónica
Se hace pasar como:	-Persona natural o jurídica
Su objetivo es obtener:	-Información personal -información confidencial. -Credenciales de inicio de sesión. -Obtener Nº de tarjeta de crédito

2.3. Definición de términos básicos

- **Datos informáticos**

Covenio (2001). Incluirá todas las representaciones de hechos, información o conceptos expresados en cualquier forma que se dé al tratamiento de la información, incluidos los programas creados para garantizar que un sistema de información realice una función.

- **Datos relativos al tráfico**

Covenio (2001). Se entenderá por tal toda información relativa a una comunicación realizada a través de un sistema de información, creada por éste como componente del plan de comunicación, que incluya el origen, destino, ruta, hora, fecha, duración y tamaño de la comunicación, o el tipo de servicio subyacente.

- **Proveedor de servicios**

Covenio (2001). Toda entidad pública o privada que proporcione a sus usuarios la capacidad de comunicarse a través de un sistema de información, así como cualquier otra organización que maneje o almacene información para ese servicio de comunicación o sus usuarios.

- **Sistema informático**

Covenio (2001). Es cualquier dispositivo independiente o grupo de dispositivos conectados o relacionados entre sí cuya función, o la de uno de sus componentes, es el manejo automatizado de datos durante la ejecución del programa. Este sistema permite procesar información de manera eficiente y confiable, facilitando la realización de tareas complejas que serían difíciles o imposibles de ejecutar manualmente.

- **Smishing**

Andina (2022). Se trata de una variante del phishing que se realiza a través de sistemas de mensajería instantánea y mensajes de texto (SMS).

- **Vishing:** Modalidad de fraude en la que se utiliza la vía telefónica para engañar al usuario, con el objetivo de obtener información personal o confidencial sin que este perciba que está siendo víctima de una estafa.

2.4. Formulación de hipótesis

2.4.1. Hipótesis general

- El desarrollo de los delitos informáticos en el sistema penal peruano en los años, 2020 a 2022, se encuentra en constante cambio.

2.4.2. Hipótesis específicas

- El desarrollo de los delitos informáticos en el sistema general del Código Penal peruano del 1991, en los años, 2020 a 2022, de modificaciones y derogaciones constante.
- El desarrollo de los delitos informáticos mediante leyes especiales Nº 30096 modificado por Ley Nº 30171 en los años, 2020 a 2021, se especializa dejando el sistema ordinario.

2.5. Variables

2.5.1. Identificación de las variables

Se ha identificado una sola variable en el contexto del sistema penal peruano, en razón de que es una investigación descriptiva que revelara datos, confirmando la hipótesis.

Variable X: Delito Informático en el sistema penal peruano

Dimensiones:

- X1: Como delito ordinario
- X2: Como delito especial

2.5.2. Definición conceptual de la variable

Bramont-Arias (1997). Se considera delito a toda acción, típica, antijuridica y culpable que “para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos.

2.5.3. Definición operacionalización de la variable

Los delitos informáticos, en el sistema penal peruano, se desarrolla como delitos ordinarios dentro del Código Penal y como delitos Especiales mediante una ley especial. Los delitos ordinarios comprenden aquellas conductas ilícitas tradicionales que se cometen utilizando medios tecnológicos, como el fraude o la estafa electrónica, mientras que los delitos especiales abarcan conductas directamente relacionadas con la tecnología de la información, como el acceso indebido a sistemas informáticos, la difusión de malware o el ciberacoso.

Esta distinción permite al sistema judicial peruano abordar de manera más efectiva las diversas modalidades de criminalidad digital, adaptando las sanciones y procedimientos a la complejidad de los hechos.

Además, la existencia de normas específicas busca proteger no solo a las personas, sino también a las organizaciones y al Estado, frente a los riesgos que representan las nuevas formas de criminalidad que surgen con el avance tecnológico.

Tabla 3. *Operacionalización de las variables*

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Delito Informático en el sistema penal peruano	Se considera delito a toda acción, típica, antijuridica y culpable que "para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos (Bramont-Arias, 1997).	Los delitos informáticos, en el sistema penal peruano, se desarrolla como delitos ordinarios dentro del Código Penal y como delitos Especiales mediante una ley especial.	**X1:** Ley Nº 30096 modificado por Ley Nº 30171.	**X1.1.** Delito contra el sistema informática. X1.2. Delitos informáticos contra la indemnidad sexual y libertad sexual. X1.3. Delitos informáticos contra la intimidad y secreto de las comunicaciones. X1.4. Delitos informáticos contra el patrimonio. X1.5. Delitos informáticos contra la fe pública.	- Eficiente - Poco eficiente - Ineficiente
			X2: Código Penal de 1991.	X2.1 Hurto telemático, art.186. X2.2. Delito informático Ley Nº 27309. X2.3. Turismo sexual infantil -Ley Nº 28251. X2.4. Clonación o adulteración de terminales de telefonía celular. X2.5. Apología al terrorismo. D. Leg. Nº 982. X2.6. Delito de propiedad intelectual, Ley Nº 29263. X2.7. Ingreso y sabotaje a centros de reclusión. Ley 29867	

Fuente: *Elaboración propia*

CAPÍTULO III

METODOLOGÍA

3.1. Diseño de investigación

- **Método general**

Se empleó el método inductivo y deductivo o análisis y síntesis, histórico y hermenéutico. Método inductivo según Egg (1995) “Es el proceso de tomar casos específicos y usarlos para sacar conclusiones generales o leyes que expliquen un fenómeno” (p. 200), el mismo autor, opina sobre el método deductivo, como “La idea de que el conocimiento general se eleva al ir más allá de los casos específicos”. (p. 98)

- **Tipo de la investigación**

Es una investigación de tipo básica o teórica, que se caracteriza por ser naturalista, fenomenológica, interpretativo (Paucar, 2020), tambien conocido de enfoque cualitativo que según Hernandez, Fernández, & Baptista (2014) es una investigación de mayor profundidad, de significados, amplitud de analisis, riqueza interpretativa y contextualizada.

- **Nivel de la investigación**

El nivel de investigación que se utilizó fue descriptivo, porque se describió el fenómeno de los delitos informáticos que se desarrolla en el sistema penal peruano, un análisis temático documental oficial y no oficial, con una técnica interpretativa de los contenidos.

- **El diseño de investigación**

El estudio fue de diseño no experimental, debido a que es interpretativo, observando los documentos en su estado natural, sin alterar el contenido.

Para Hernandez et al. (2014). “La investigación no experimental son estudios que se realizan sin la manipulación deliberada de las variables en estudio

y en los que sólo se observan los fenómenos en su ambiente natural para analizarlos" (p. 185)

3.2. Población y muestra

3.2.1. Población

La población que formó parte de esta investigación fueron los fiscales de las cinco fiscalías provinciales penales corporativas de coronel portillo, que están integrados cada uno, un titular y tres adjuntos, que en total suman 20 integrantes.

3.2.2. Muestra

La muestra que conformó el presente estudio, debido al tamaño de su población, incluyó a todos los integrantes. Es decir, se eligió mediante el método probabilístico, considerando que la población es pequeña y no requiere para su evaluación el uso de una fórmula específica. Esta decisión permitió que los resultados reflejaran de manera más precisa las características del grupo estudiado, garantizando así la validez y representatividad de los datos obtenidos.

3.3. Técnicas e Instrumentos de recolección de datos

3.3.1. Técnica

La técnica de investigación fue la entrevista dado que nos permitirá obtener información de manera directa para posteriormente someter a un análisis por objetivos.

3.3.2. Instrumento

Para el proceso de recolección de datos utilizamos el cuestionario con la que obtuvimos los datos respecto a las variables de estudio.

3.4. Validación y confiabilidad del instrumento

La validación de los instrumentos se llevó a cabo mediante la opinión de expertos, especialmente docentes de la Universidad Nacional de Ucayali, y la confiabilidad se determinó utilizando el sistema SPSS. Esto permitió garantizar

que los instrumentos fueran adecuados, precisos y consistentes para la recolección de datos del estudio.

3.5. Técnicas para el procesamiento de la información

- **Procedimiento de recolección de datos**

Se presentaron los datos recolectados en tablas estadísticas, ya que, al ser una investigación cualitativa se trabajará por porcentajes en la cual se seguirá el siguiente procedimiento.

El primer paso, se inició buscando información bibliográfica para ampliar los conocimientos en cuanto a las variables de estudio.

El segundo paso se procedió a elaborar los instrumentos de investigación.

El tercer paso se efectuó la aplicación del instrumento de investigación, **Finalmente** se realizó la prueba de hipótesis y plantearemos la discusión, conclusión y recomendación de la investigación.

Los resultados obtenidos se presentan en figuras y tablas, cada una de ellas analizada con el propósito de examinar la relación entre las variables del estudio.

CAPÍTULO IV

RESULTADOS Y DISCUSIONES

4.1. Descripción de resultados

Tabla 4

Entrevista número Uno – realizados a los Fiscales

Nº de entrevistados	A su parecer ¿Cuál es el nivel de desarrollo del delito contra el sistema informático en el sistema penal peruano, eficiente, poco eficiente o ineficiente?
E 1	Es ineficiente: porque el nivel es abismal en las últimas décadas, especialmente a medida que las tecnologías digitales han avanzado y el cibercrimen se ha vuelto más sofisticado, este delito abarca conductas como el acceso no autorizado la interferencia en datos o sistemas, y el uso indebido de tecnologías con fines ilícitos.
E2	Es poco eficiente: porque ha evolucionado en respuesta al aumento de la digitalización y la creciente incidencia de ciberdelitos, y la Ley 30171 ley de delito informáticos regulan de manera especifico cada conducta hecha delito en relación a utilización tecnológica.
E3	Es ineficiente: Es muy limitado mucho de los delitos informáticos son ejecutados por personas muy hábiles en la tecnología y la normativa actual solo prevé 3 artículos.
E4	Es ineficiente: En este punto el C.P. la tipifica como delitos informáticos en la cual la pena se encuentra insólito al convenio, y este delito es de todos los días a nivel nacional.
E5	Es ineficiente: porque el nivel del delito es alto, el uso de la tecnología digital ha ido en aumento y la delincuencia cibernética ha ido mejorando.
E6	Es poco eficiente a pesar su nivel de desarrollo varía dependiendo de la gravedad del delito e incluye penas de prisión que van desde 1 hasta 10 años, dependiendo de los efectos del delito y si hubo daños o perjuicios económicos.
E7	Es ineficiente porque el marco normativo todavía enfrenta dificultades para cubrir la complejidad de los delitos informáticos especialmente en el ámbito de la cibercriminalidad.
E8	Es eficiente porque su desarrollo ha progresado consideradamente gracias a la ley 30096nque establece un marco normativo moderno y alineado con estándares internacionales. sin embargo, es necesario seguir fortaleciendo las capacidades institucionales promoviendo la educación en ciberseguridad a los agentes especializados.
E9	Es eficiente porque su desarrollo ha avanzado notablemente con la Ley 30096 tipifica diversas conductas ilícitas relacionados con la ciberdelincuencia esta ley establece sanciones para delitos como el acceso ilícito, el fraude informático y la alteración de datos con penas de 1 o 8 años.
E10	Es eficiente porque los delitos informáticos se conducen por su propia ley. en nuestro país hay un incremento de vulneración de los sistemas informáticos, lo que debe ser de atención para los legisladores, para implementar la normatividad vigente.
E11	Es ineficiente porque el delito tiene un nivel elevado.
E12	Es poco eficiente porque actualmente se ve una gran evolución de estos tipos de delitos informáticos.
E13	Es ineficiente el desarrollo porque el nivel de los hechos es enorme, ya que los delitos informáticos incluyen actos que comprometen integridad confidencialidad o disponibilidad de los sistemas informáticos como el hacker, ataques de denegación de servicios y la intercepción ilícita.
E14	A nivel de tipificación es eficiente ya que la normativa esta promulgada el 2013, ha sido actualizada para adaptarse a las normas modalidades delictivos que según con el avance tecnológico, según datos de 2019, se registran 3,012 de delitos informativos en Perú, con un notable aumento en los fraudes informáticos, que alcanzaron 2,097 casos.
E15	Su nivel de desarrollo de la ley en los delitos informáticos en poco eficiente debido a que los delincuentes no son identificados.
E16	Es ineficiente porque la ley es muy limitada, al enfrentar el delito en el campo real.
E17	Es eficiente porque la ley se ha ido actualizando paulatinamente
E18	Es ineficiente porque los delitos informáticos quedan impunes por falta de tipicidad o falta de logística.
E19	Es poco eficiente porque los delitos y los hechos informáticos van en aumento y la ley no recoge todos los casos en su tipicidad.
E20	Es eficiente porque el legislador ha ido adecuado a la realidad los delitos informáticos.

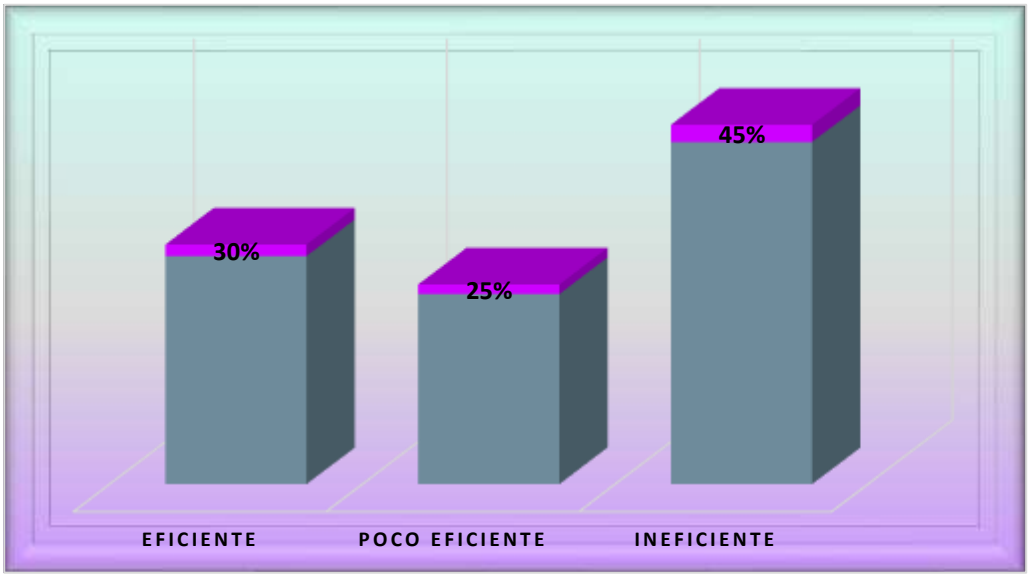
Tabla 5

Resultados de Entrevista número Uno – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	6	30%
Poco eficiente	5	25%
Ineficiente	9	45%
TOTAL	20	100%

Figura 1

Resultados de Entrevista número Uno – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los fiscales se obtuvo como resultado que un 30 % de nuestra muestra nos indican que es EFICIENTE el nivel de desarrollo del delito contra el sistema informático en el sistema penal peruano, un 25% nos indican que es POCO EFICIENTE pero un buen porcentaje indican que es INEFICIENTE con un 45%.

Tabla 6

Entrevista número Dos – realizados a los Fiscales

Nº de entrevistados	Según su apreciación ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la indemnidad sexual y libertad sexual en el sistema penal peruano, es eficiente, poco eficiente y ineficiente?
E 1	Es poco eficiente: El nivel de desarrollo sobre este delito es abrumador, pero se encuentra regulado en la ley Nº 30096 que establece un marco legal para prevenir y sancionar conductas ilícitas que afectan tanto a sistema informático como derechos de libertad de los delitos informáticos que afectan la indemnidad y la libertad sexual.
E2	Es ineficiente: porque es un tema en constante evolución impulsado para el uso generalizado de tecnología y la aparición de nuevas modalidades delictivas.
E3	Es poco eficientes: porque es muy bajo, en la ley Nº 30096, se prevé 2 artículos los cuales no son suficientes para lograr la protección integral del bien jurídico protegido en este delito.
E4	Es ineficiente, porque el desarrollo de este delito es precario, en razón de su complejidad.
E5	Es poco eficiente porque esto ha ido evolucionando, debido al uso de la tecnología, la aparición de nuevos redes sociales y aplicativos móviles.
E6	Es ineficiente porque hay limitaciones en la capacitación de los operadores de justicia la actualización tecnológica y la colaboración con plataformas digitales.
E7	Es poco eficiente: porque a pesar de contar con normativa especializada la normativa peruana ha logrado adaptarse a las normas tecnológicas, protegiendo la privacidad y el secreto de privacidad sexual.
E8	Es eficiente porque su desarrollo es significativo, pero enfrenta desafíos en su aplicación práctica a través de la ley 30096 y reformas posteriores al C.P. se han tipificado conductas como la difusión no consentida de material íntimo, el acoso sexual virtual, y la captación por medios tecnológico con fines sexuales.
E9	Es eficiente porque el desarrollo tuvo un avance con la incorporación de la ley 30096 y sus modificaciones para delitos como la difusión no autorizada de contenido sexual y el acoso cibernético reflejando un compromiso por proteger a los victimas especialmente a menores.
E10	Es poco eficiente porque su incidencia va al incremento en conjunto con el avance de la ciencia tecnología y por ende los sistemas informáticos, la practicidad del internet facilita a sus usuarios de acceder a paginas creadas directamente para publicitar servicios.
E11	Es ineficiente porque el nivel es muy alto en cuanto a su castigo a los responsables
E12	Es poco eficiente porque estos delitos afectan gravemente los derechos de las personas menores de edad abarca conductas como el groming la pornografía infantil y el sex ting no consentido, los delitos informáticos contra la indemnidad y libertad sexual.
E13	Es ineficiente porque su desarrollo es bastante preocupante.
E14	Es ineficiente, porque no tiene mucho apoyo por parte de las leyes, que solo 2 art. Amparan a estos delitos.
E15	Es poco eficiente porque cada vez va en aumento considerable que ya no se puede controlar.
E16	Es eficiente porque este delito está regulado en la ley 30096, donde indica cómo prevenir y sancionar conductas ilícitas, que involucra y afecta al sistema informático donde se tipifica específicamente: proposiciones a niñas y niños y adolescentes, con fines sexuales, intercepción de datos informáticos y suplantación de identidad.
E17	Es poco eficiente porque los delitos contra la indemnidad sexual sus incidencias son muy alta en menores de edad.
E18	Es poco eficiente porque los hechos detectados sobre delitos contra la indemnidad sexual son de mínima efectividad.
E19	Es poco eficiente porque su nivel es moderado, de los delitos contra la indemnidad sexual.
E20	Es poco eficiente porque es moderado, ya se puede controlar su desarrollo con la Ley Nº 30096.

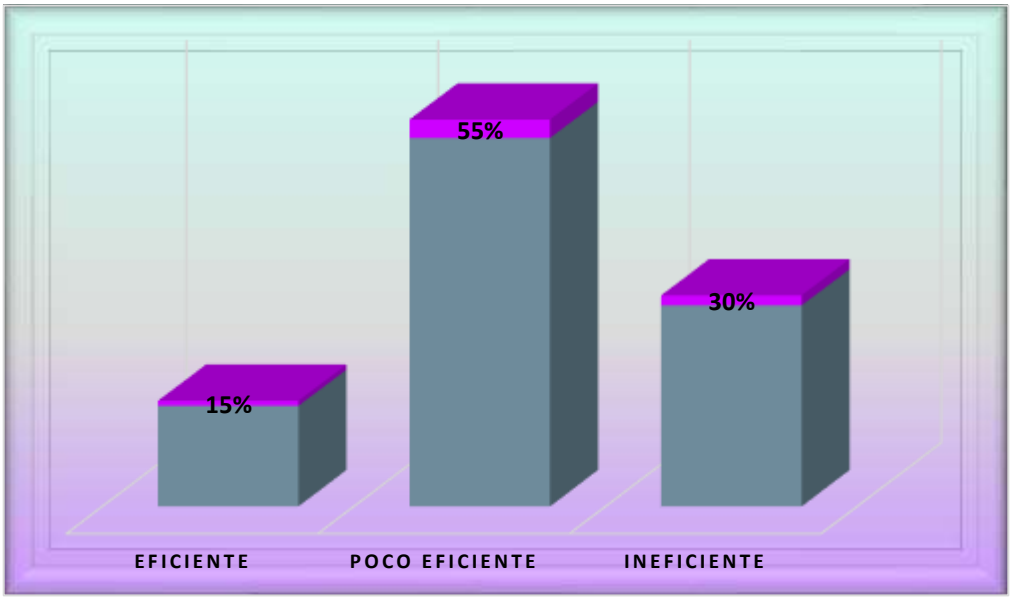
Tabla 7

Resultados de Entrevista número Dos – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	3	15%
Poco eficiente	11	55%
Ineficiente	6	30%
TOTAL	20	100%

Figura 2

Resultados de Entrevista número Dos – realizados a los Fiscales



Interpretación: De las entrevistas hechas a los fiscales se tuvo como resultado que un 15% de entrevistadas indican que es EFICIENTE el nivel de desarrollo de los delitos informáticos contra la indemnidad sexual y libertad sexual en el sistema penal peruano, pero un porcentaje considerable de 55% de entrevistados indican que es POCO EFICIENTE; así mismo un 30% indican que es INEFICIENTE.

Tabla 8

Entrevista número Tres – realizados a los Fiscales

Nº de entrevistados	Según su opinión ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la intimidad y secreto de las comunicaciones en el sistema penal peruano, eficiente, poco eficiente e ineficiente?
E 1	Es poco eficiente: porque el desarrollo es significativo en los últimos años, reflejando un aumento en la preocupación por la seguridad digital y la protección de datos personales, la ley 30096 regula estos delitos con especificaciones como la intercepción.
E2	Es eficiente porque en su evolución fue y ha sido significativamente en los últimos años en respuesta al uso masivo de tecnología de información y comunicación y afecta conductas y derechos fundamentales como la privacidad.
E3	Es ineficiente porque es muy bajo, pues se prevé solo un artículo en la ley 30096, llevado a la realidad existen más acciones que la prevista en dicha ley, puede que la tecnología siempre es más avanzada que la ley.
E4	Es poco eficiente porque el nivel de desarrollo es mínimo, toda vez que existen nuevas modalidades de delitos informáticos.
E5	Es eficiente porque su nivel ha sido alto, esto es ah demanda de los medios tecnológicos para la obtención de información privada de los usuarios.
E6	Es poco eficiente porque en el sistema penal peruano aun presenta limitaciones en la prevención y sanción de los delitos informáticos contra la intimidad y el secreto de las comunicaciones.
E7	Es poco eficiente porque el nivel es intermedio ya que la legislación a comenzado a aprobar estos delitos y a la práctica aun presenta desafíos.
E8	Es poco eficiente porque su desarrollo es moderado en cuanto a tipificaciones y sanciones a través, de la ley 30096 y sus reformas en el C.P. esta base normativa es adecuado para abordar estos delitos, pero el nivel de desarrollo practico aún es insuficiente para garantizar una protección efectiva de la intimidad y el secreto de las comunicaciones.
E9	Es eficiente porque el desarrollo de estos delitos y su nivel es paulatinamente especial con la tipificación de conductas como el acceso no autorizado a sistemas informáticos y la interceptación de datos, estableciendo penas que varían entre 1 a 8 años prisión.
E10	Es eficiente porque es moderado, si bien ambas figuras se relacionan en cuanto a la privacidad de la información personal, ambas tienen su conducta regular diferenciado.
E11	Es eficiente porque es significativo su avance.
E12	Es poco eficiente porque es muy bajo, pues se prevé solo un artículo en la ley 30096
E13	Es eficiente porque el nivel es alto; más aún en estos tiempos con el avance tecnológico es fácil de jaquearte, el Messenger, whashap, Instagram o cualquier red.
E14	Es eficiente porque es significativo
E15	Es eficiente porque el desarrollo es alto.
E16	Es eficiente porque su desarrollo es significativo en el ámbito legislativo.
E17	Es poco eficiente porque el nivel es moderado en su avance.
E18	Es poco eficiente porque el sistema penal peruano aun presenta limitaciones
E19	Es ineficiente porque es muy bajo, pues se prevé solo un artículo en la ley 30096, que no abarco en su conjunto.
E20	Es eficiente porque es poco significativo su avance.

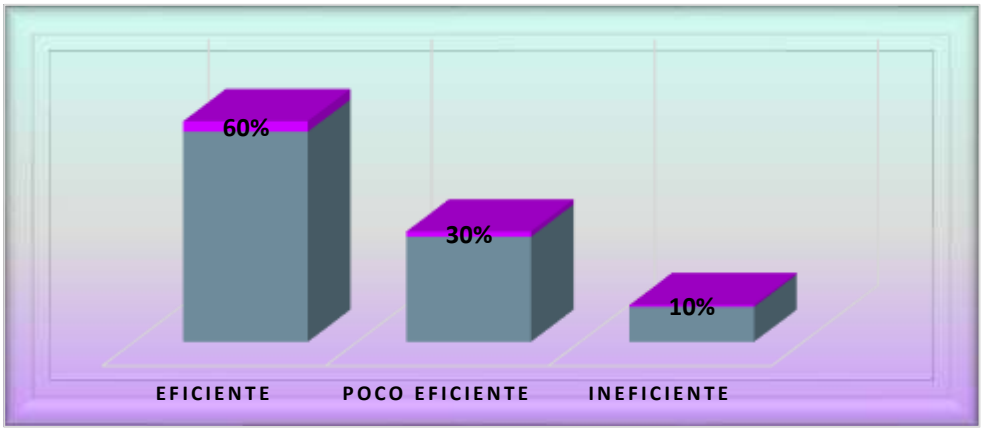
Tabla 9

Resultados de Entrevista número Tres – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	12	60%
Poco eficiente	6	30%
Ineficiente	2	10%
TOTAL	20	100%

Figura 3

Resultados de Entrevista número Tres – realizados a los Fiscales



Interpretación: Según la pregunta ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la intimidad y secreto de las comunicaciones en el sistema penal peruano?, se obtuvo como resultados que el 60% de entrevistados consideraron que es EFICIENTE el nivel de desarrollo de los delitos informáticos contra la intimidad y secreto de las comunicaciones en el sistema penal peruano; el 30% es POCO EFICIENTE, pero sin embargo un 10 % indican que es INEFICIENTE.

Tabla 10

Entrevista número Cuatro – realizados a los Fiscales

Nº de entrevistados	¿Cuál es el nivel de desarrollo de los delitos informáticos contra el patrimonio en el sistema penal peruano, eficiente, poco eficiente o ineficiente?
E 1	Es eficiente porque en relación al patrimonio se formaliza con la aprobación de la ley 30096 que tiene como objeto prevenir y sancionar conductas ilícitas que afectan sistemas y datos informáticos, así como otros bienes jurídicos.
E2	Es eficiente porque su desarrollo tuvo un avance considerablemente, reflejándose en la en la adecuación de marco normativo que abarca la conducta que afecta que afecta bienes económicos utilizando tecnología alguno de ellos es muy común: fraude informático, pishing, skimming.
E3	Es poco eficiente porque es muy bajo su respuesta, si bien en la ley 30096, se prevé el delito contra el patrimonio por delitos informáticos, pero solo se implementó dos art. Y no es suficiente con ello buscar protección a los bienes patrimoniales.
E4	Es ineficiente porque ocurre lo mismo cuando no estaba vigente el nivel es muy bajo.
E5	Es poco eficiente porque su nivel ha ido en aumento, esto gracias a la utilización de entrarnos digitales donde se hace las transferencias de los bienes.
E6	Es poco eficiente porque el sistema penal peruano aún enfrenta dificultades para para abordar de manera efectiva los delitos informáticos contra el patrimonio.
E7	Existen deficiencias en la capacitación de las autoridades y en los recursos disponibles para la investigación de estos delitos.
E8	Es poco eficiente porque su desarrollo es intermedio con avances normativos significativos, pero con limitaciones prácticos en su implementación como la tipificación del delito de fraude informático, el phishing y la manipulación indebida de sistema de pago, estableciendo penas severas, pero sin llegar autor del delito.
E9	Es poco eficiente porque su desarrollo es significativo más aun con la tipificación del fraude informático y otras conductas sin embargo se ha identificado que la legislación presenta deficiencias ya que agrupa diversas modalidades de delitos bajo un mismo concepto, lo que genera confusión.
E10	Es ineficiente porque la ciberdelincuencia va en aumento y es complicado determinar incluso el medio intelectual de la comisión de un delito se requiere área y personal especializado a nivel nacional y no solo un área para atención nacional.
E11	Es eficiente porque su desarrollo tuvo un avance considerado, ya que el estado ha establecido regulaciones para sancionar delitos que utilizan la tecnología para su ejercicio, a base de la Ley 29733 ley de protección de datos personales.
E12	Es eficiente porque su desarrollo ha ido evolucionando paulatinamente.
E13	Es poco eficiente porque su desarrollo es intermedio.
E14	Es ineficiente porque el nivel es bajo, ya que ampara dos artículos y no es severa su castigo.
E15	Es ineficiente porque cada vez es más considerable estos tipos de delitos, porque quedan impunes.
E16	Es ineficiente porque su nivel realmente alarmante.
E17	Es poco eficiente porque el nivel es moderado.
E18	Es poco eficiente porque la ley 30096 clasifica varios delitos informáticos entre los cuales destacamos los delitos contra el patrimonio. Uno de los principales delitos es el fraude informático, que se define como la obtención de un beneficio ilícito para uno mismo mediante la manipulación de datos informáticos.
E19	Es ineficiente porque este tipo de delitos va en aumento.
E20	Es ineficiente debe haber más leyes que sancionen severamente, se nota la evolución.

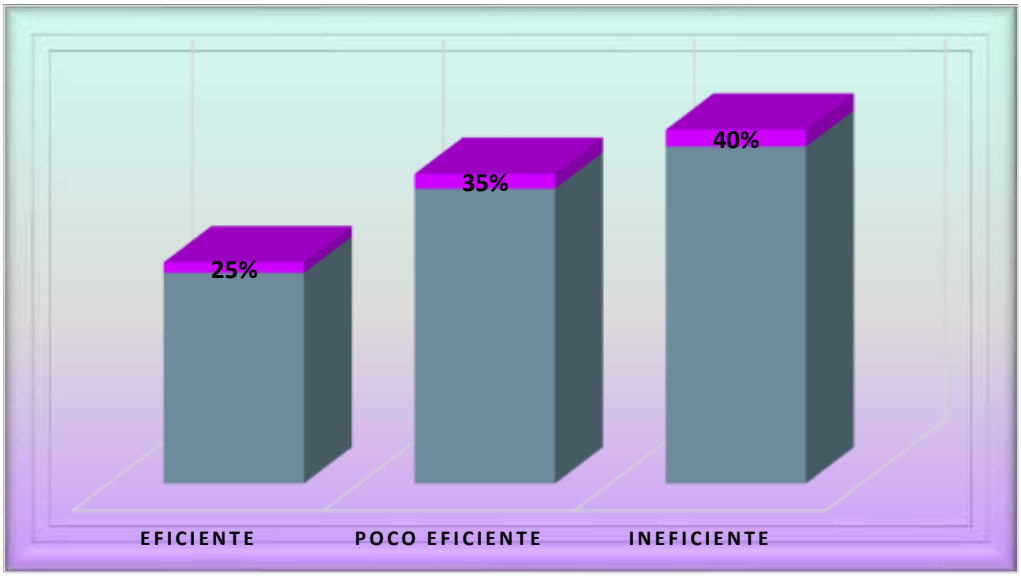
Tabla 11

Resultados de Entrevista número Cuatro – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	5	25%
Poco eficiente	7	35%
Ineficiente	8	40%
TOTAL	20	100%

Figura 4

Resultados de Entrevista número Cuatro – realizados a los Fiscales



Interpretación: De las entrevistas realizados a los señores fiscales, se obtuvo como respuesta que un 25% de consultantes indican que es EFICIENTE el nivel de desarrollo de los delitos informáticos contra el patrimonio en el sistema penal peruano, eficiente, poco eficiente o ineficiente; el 35% indican que es POCO EFICIENTE pero el mayor porcentaje con un 40% indican que es INEFICIENTE el nivel de desarrollo.

Tabla 12

Entrevista número Cinco – realizados a los Fiscales

Nº de entrevistados	A su opinión: ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la fe pública en el sistema penal peruano, eficiente, poco eficiente o ineficiente?
E 1	Es eficiente porque su desarrollo es muy significativo ya que los delitos informáticos afectan directamente la fe pública al comprometer la confianza en las transacciones digitales y en la integridad de los datos y documentos digitales que hoy en día utiliza las diversas instituciones públicas.
E2	Es eficiente porque en desarrollo cobra más notoriedad especialmente en la promulgación de la Ley Nº 30096 (Ley de delitos informáticos) y las reformas del C:P.
E3	Es poco eficiente: Es relativamente bajo, el estado hasta la actualidad no se ha centrado en la creación integral de normativas que prevean estos delitos, si bien existen fiscalía de ciberdelincuencia, pero no se ha implementado en todo el país, solo se ha implementado en todo el país solo se ha centralizado en lima y no en provincia.
E4	Es ineficiente porque es pésimo a nivel nacional.
E5	Es ineficiente porque el nivel es bajo por la naturaleza del delito
E6	Es poco eficiente porque la legislación aun no adapta completamente a la rapidez evolución de las tecnologías y las formas sofisticadas de ciberdelincuencia digital de documentos oficiales y las alteraciones de registros.
E7	Es poco eficiente porque se encuentra en un nivel intermedio, ya que se necesita un mayor esfuerzo en la actualización constante de las normativas y en la capacitación de las autoridades hacer frente a las nuevas modalidades de ciberdelincuencia.
E8	Su capacidad es nulo o incipiente con avances normativos importantes pero una implementación limitada, a través de la ley 30096, el sistema penal a incorporado disposiciones como la falsificación de documentos informáticos, y el uso indebido de medios electrónicos.
E9	Es eficiente porque la fe pública como la suplantación de identidad con relación a sistemas informáticos reflejan una significativa avance en cuanto a la ciberdelincuencia, pero la efectividad de las sanciones contra los autores es casi nula por no contar una fiscalía especializada en conductas ilícitas utilizando medios informáticos.
E10	Es poco eficiente porque no tiene modificación vigente su normatividad se mantiene en relación a los delitos informáticos este capítulo es vulnerable en la actualidad no tiene mayor incidencia.
E11	Es ineficiente porque su aplicación es muy bajo.
E12	Es poco eficiente porque es moderado el nivel de aplicación.
E13	Su desarrollo va en aumento, y es preocupante.
E14	Es ineficiente porque su aplicación es pésima.
E15	Es eficiente porque el nivel es elevado en la tipificación.
E16	Es ineficiente porque su desarrollo es paulatino y no combate la delincuencia.
E17	Es poco eficiente el desarrollo de este delito.
E18	Es poco eficiente por decir su desarrollo es muy moderado.
E19	Moderado.
E20	Es ineficiente porque su desarrollo es de nivel nulo más aun en nuestra región que no cuenta con una fiscalía especializada por lo cual los delitos son vistos por fiscales de tuno.

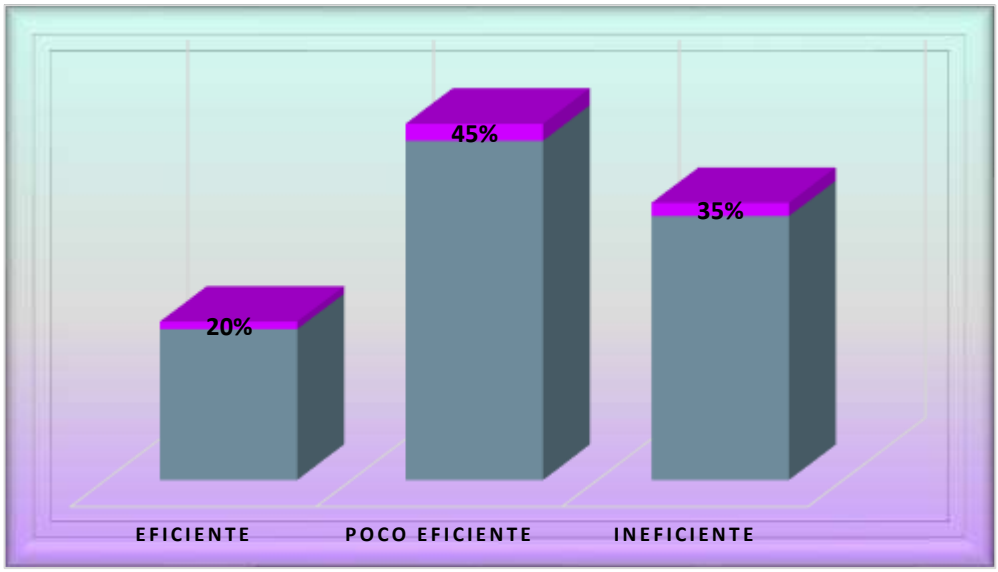
Tabla 13

Resultados de Entrevista número Cinco – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	4	20%
Poco eficiente	9	45%
Ineficiente	7	35%
TOTAL	20	100%

Figura 5

Resultados de Entrevista número Cinco – realizados a los Fiscales



Interpretación: De las entrevistas realizados a los señores fiscales se obtuvo como respuesta que un 20% de entrevistados respondieron que es EFICIENTE el nivel de desarrollo de los delitos informáticos contra la fe pública en el sistema penal peruano; el 45% de entrevistados indican que es POCO EFICIENTE, finalmente el 35% indican que es INEFICIENTE el nivel de desarrollo.

Tabla 14

Entrevista número Seis – realizados a los Fiscales

Nº de entrevistados	A su opinión: ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal?
E 1	Es eficiente porque en su momento su evolución fue significativo relacionado con la promulgación de la Ley Nª 30096, esta ley se introdujo para abordar de manera efectiva los delitos que involucran el uso de tecnología de la información y comunicación, su evolución se originó en el art. 186 del CP, donde se establecido de 3 a 6 años cuando el hurto se realizaba a través de la transferencia electrónica, la cual fue derogada con la Ley Nª 30096.
E2	Es eficiente porque el hurto telemático se incorporó en el art. 186 del CP su desarrollo se realiza mediante la aprobación ilícita de bienes o activos mediante el uso de tecnologías de la información y comunicación su desarrollo se centra del acceso al internet.
E3	Es poco eficiente porque el art.186 que se hace referencia prevé el delito de hurto agravado, mediante el delito telemático.
E4	Es deficiente porque el desarrollo es precario por falta de tecnología.
E5	Es eficiente porque en su momento este delito se incorporó en el art. 186 del CP y se desarrolla mediante la apropiación ilícita de bienes con el uso de la tecnología de la información y la comunicación.
E6	Es poco eficiente porque su desarrollo del hurto telemático es limitado carece de acceso a plataformas digitales, sino que también influyen al acceso no autorizado a sistemas de información o la manipulación de datos para obtener beneficios ilícitos.
E7	Es poco eficiente porque el hurto telemático son delitos informáticos con dificultad en nuestro sistema en cuanto a las pruebas electrónicas, ya que las autoridades judiciales y policiales han tenido que adaptarse a nuevas tecnologías de investigación.
E8	Es eficiente porque el hurto telemático, tipificado en el art. 186 del C.P. ha evolucionado en su desarrollo dentro del sistema jurídico nacional específicamente a raíz de la creciente incidencia del delito informático.
E9	Es eficiente porque se ha desarrollo a evolución con la promulgación de la ley 30096 sobre especialmente el delito de hurto telemático y lo derogo y lo estableció como fraude informático como delito autónomo protegiendo patrimonio mediante la manipulación de sistema informático.
E10	Es poco eficiente porque en el art. 186 del C.P. se encuentran las circunstancias agravantes del tipo penal consistente en el delito de hurto. no obstante, se aprecia en el numeral 7) del segundo párrafo respecto al delito cometido en relación de las telecomunicaciones empero emerge de un recurso natural, patrimonio del estado, donde no se evidencia mayor incidencia en el delito informático.
E11	Es ineficiente porque su desarrollo es bastante alarmante, porque el hurto telemático va en aumento a nivel nacional.
E12	Es eficiente porque precario el desarrollo de la legislación, debido a que la tecnología no para de producir nuevos artefactos, sobre el intercambio comercial.
E13	Es eficiente porque su desarrollo ha evolucionado, significativamente para enfrentar este delito, sin embargo, la implementación para identificar y sancionar todavía no.
E14	Es eficiente porque es significativo el desarrollo del hurto telemático en nuestro sistema penal.
E15	Es ineficiente porque no tiene mucha relevancia por falta de tecnología de punta para hacer frente a estos tipos de delitos.
E16	Es eficiente porque ha evolucionado, el hurto telemático, tipificado en el art. 186 del C.P.
E17	Es poco eficiente porque su desarrollo es moderado del hurto telemático, debido a que la tecnología sigue en desarrollo.
E18	Es poco eficiente porque su desarrollo es moderado porque la tecnología continua con su desarrollo que de seguro surgirán nuevos elementos.
E19	Es eficiente su desarrollo porque están tipificados en diferentes partes del Código Penal, por ejemplo, En el art. 186 del C.P. se encuentran las circunstancias agravantes del tipo penal consistente en el delito de hurto. no obstante, se aprecia en el numeral 7) del segundo párrafo respecto al delito cometido en relación de las telecomunicaciones empero emerge de un recurso natural.
E20	Es ineficiente porque el delito telemático no tiene desarrollo en la jurisprudencia, sin embargo, en la ley penal está tipificado.

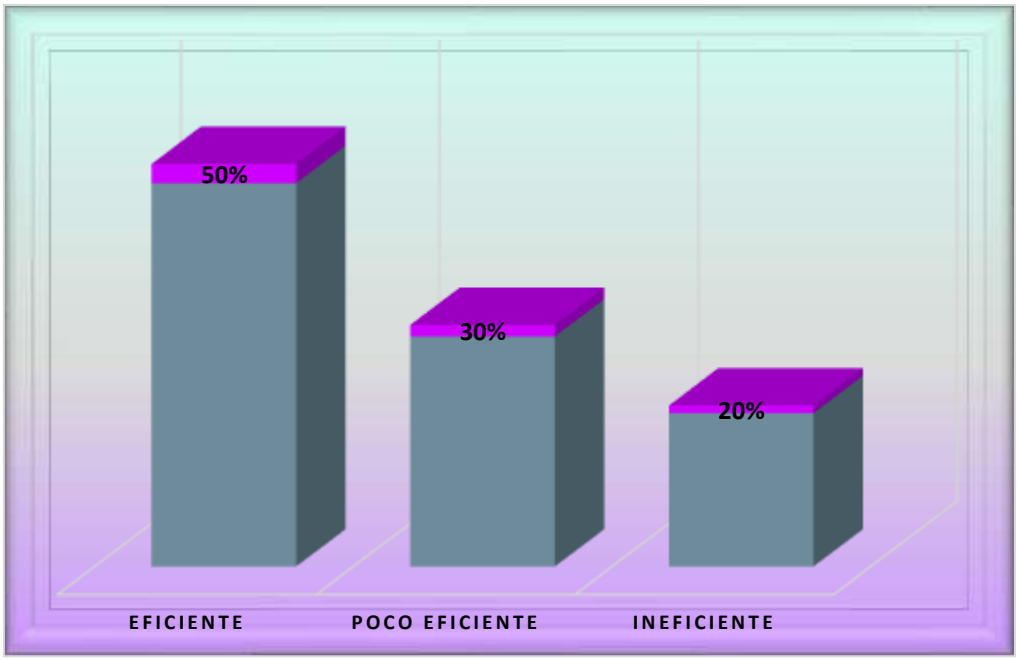
Tabla 15

Resultados de Entrevista número Seis – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	10	50%
Poco eficiente	6	30%
Ineficiente	4	20%
TOTAL	20	100%

Figura 6

Resultados de Entrevista número Seis – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los señores fiscales se obtuvo como resultado que un 50% de entrevistados indicaron que es EFICIENTE, el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal; el 30% indica que es POCO EFICIENTE sin embargo hay un 20% de entrevistados que indican que es INEFICIENTE el desarrollo en el sistema jurídico el delito de hurto telemático.

Tabla 16

Entrevista número Siete – realizados a los Fiscales

Nº de encuestados	Según su apreciación. ¿Cuál es el desarrollo en el sistema jurídico nacional los delitos de proposición a niños, niñas y adolescentes con fines sexuales, eficiente, poco eficiente o ineficiente?
E 1	Es eficiente porque está tipificado en el Art. 5 de la Ley 30096.
E2	Es eficiente porque esta sancionado por la ley Nº 30096
E3	Es poco eficiente porque los imputados no son identificados en la mayoría de los casos.
E4	Es ineficiente porque es muy bajo los resultados obtenidos.
E5	Es poco eficiente porque el delito sigue en aumento.
E6	Es poco eficiente porque no existe suficiente logística.
E7	Es ineficiente porque los resultados son poco favorables.
E8	Es eficiente porque existe una ley especial sobre delitos informáticos esta ley Nº 27309 marca un hito significativo en el sistema jurídico peruano.
E9	Es ineficiente porque los resultados suben en forma alarmante cada año.
E10	Es eficiente porque la ley va de la mano con los cambios permanentes de la tecnología.
E11	Es poco eficiente porque los resultados revelan que el delito está en aumento.
E12	Es eficiente porque existe una ley especial que sanciona los hechos.
E13	Es eficiente en cuanto a la tipificación, la ley castiga este tipo de delitos.
E14	Es poco eficiente porque la tecnología va aumentando su capacidad que le permite al delincuente escudarse en la sobra de la tecnología.
E15	Es eficiente porque da herramientas a la PNP y los fiscales perseguir el delito.
E16	Es poco eficiente porque los logros no son los más optimistas.
E17	Es ineficiente porque no ha servido de disuasión más bien va en aumento el delito.
E18	Es poco eficiente porque la promulgación de la ley no ha cambiado el escenario más bien ha aumentado.
E19	Es eficiente porque existen herramientas legales para perseguir y castigar al delincuente.
E20	Es poco eficiente por falta de logista adecuado.

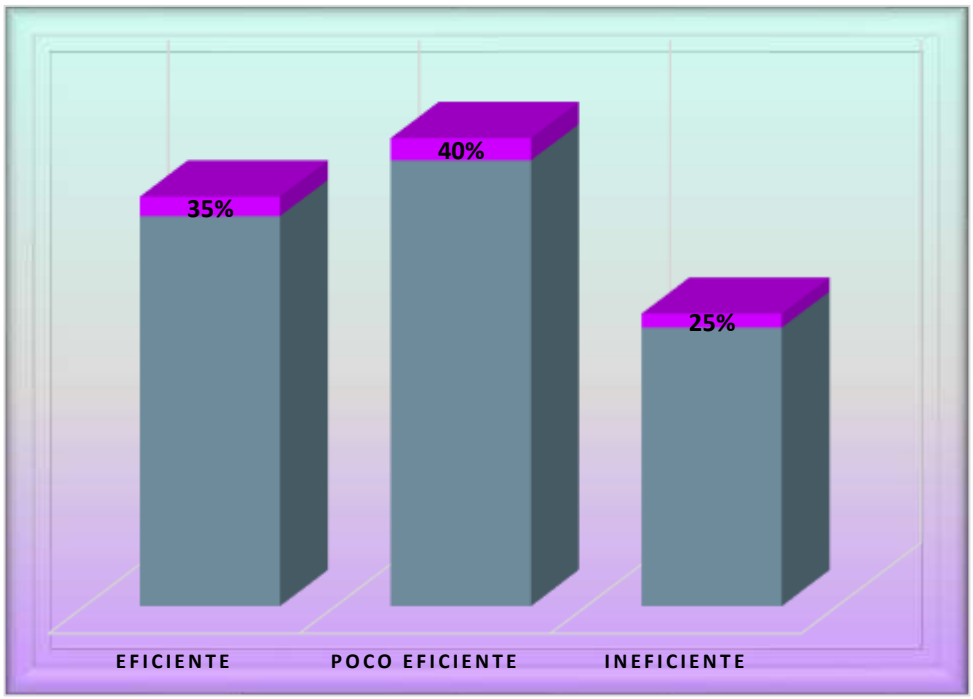
Tabla 17

Resultados de Entrevista número Siete – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	7	35%
Poco eficiente	8	40%
Ineficiente	5	25%
TOTAL	20	100%

Figura 7

Resultados de Entrevista número Siete – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los señores fiscales, se obtuvo como resultado que un 35% de entrevistados indican que es EFICIENTE el desarrollo en el sistema jurídico nacional los delitos de proposición a niños, niñas y adolescentes con fines sexuales, el 40% indican que es POCO EFICIENTE, pero hay un pequeño porcentaje de 25% que cree que es INEFICIENTE.

Tabla 18

Entrevista número Ocho – realizados a los Fiscales

Nº de Entrevistados	A su opinión: ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de interceptación de datos informáticos?
E 1	Es ineficiente
E2	Es eficiente porque existe herramientas legales para perseguir y sancionar
E3	El desarrollo en el sistema jurídico nacional del delito de interceptación de datos informáticos es poco eficiente.
E4	Es poco eficiente.
E5	Es poco eficiente
E6	Es ineficiente.
E7	Es poco eficiente.
E8	Es eficiente porque el desarrollo legal otorga herramientas para sancionar.
E9	Es poco eficiente.
E10	Es poco eficiente.
E11	Es eficiente.
E12	Es ineficiente.
E13	Es poco eficiente.
E14	Es poco eficiente.
E15	Es ineficiente.
E16	Es ineficiente.
E17	Es ineficiente.
E18	Es poco eficiente.
E19	Es poco eficiente.
E20	Es poco eficiente.

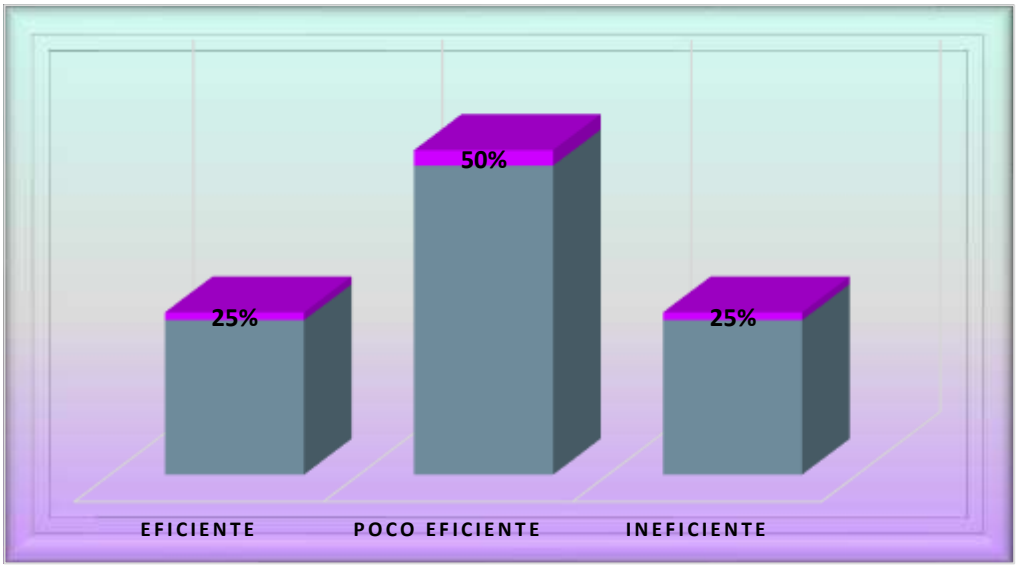
Tabla 19

Resultados de Entrevista número Ocho – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	5	25%
Poco eficiente	10	50%
Ineficiente	5	25%
TOTAL	20	100%

Figura 8

Resultados de Entrevista número Ocho – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los señores fiscales, se obtuvo como resultado que un 25% de entrevistados indican que es EFICIENTE, el desarrollo en el sistema jurídico nacional del delito de interceptación de datos informáticos indica que es POCO EFICIENTE y el otro 25% indican que es INEFICIENTE el desarrollo en este sistema.

Tabla 20

Entrevista número Nueve – realizados a los Fiscales

Nº de entrevistados	A su apreciación ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de fraude informático, eficiente, poco eficiente o ineficiente?
E 1	Es eficiente.
E2	Es eficiente.
E3	Es poco eficiente.
E4	Es poco eficiente
E5	Es deficiente.
E6	Es poco eficiente.
E7	Es poco eficiente.
E8	Es ineficiente.
E9	Es ineficiente.
E10	Es ineficiente.
E11	Es ineficiente.
E12	Es poco ineficiente.
E13	Es poco ineficiente.
E14	Es ineficiente.
E15	Es poco eficiente.
E16	Es poco eficiente.
E17	Es poco eficiente.
E18	Es poco eficiente
E19	Es ineficiente.
E20	Es eficiente.

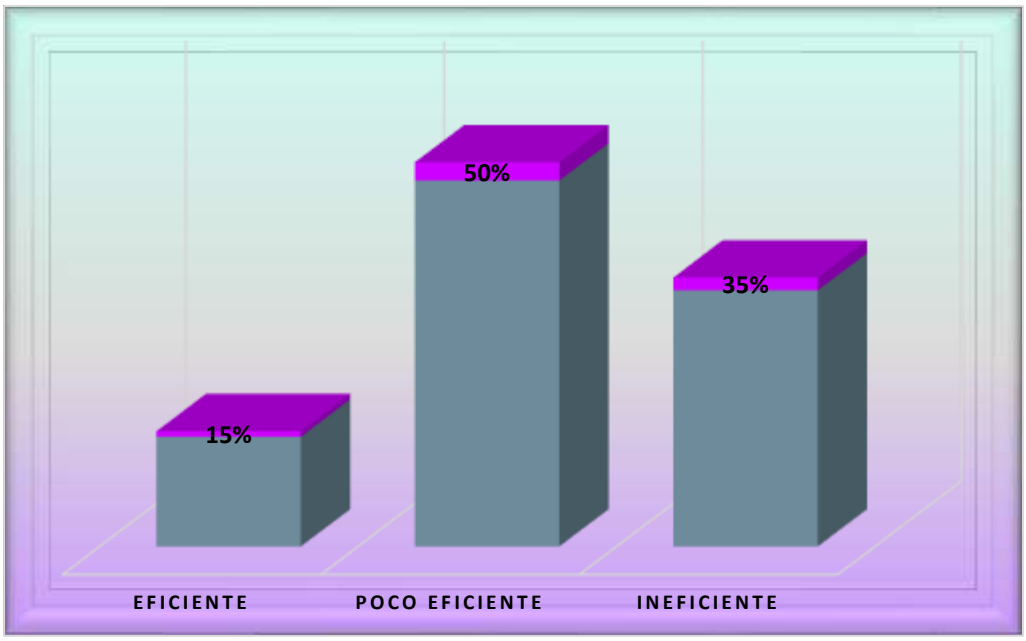
Tabla 21

Resultados de Entrevista número Nueve – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	3	15%
Poco eficiente	10	50%
Ineficiente	7	35%
TOTAL	20	100%

Figura 9

Resultados de Entrevista número Nueve – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los señores fiscales, se obtuvo como resultado que solo un 15% de entrevistados indican que es EFICIENTE el desarrollo en el sistema jurídico nacional el delito de fraude informático, el 50% de entrevistados indican que es POCO EFICIENTE pero el 35% de encuestados indican que es INEFICIENTE.

Tabla 22

Entrevista número Diez, realizados a los Fiscales

Nº de entrevistados	¿Cuál es el desarrollo en el sistema jurídico nacional el delito de suplantación de identidad?
E 1	Es eficiente
E2	Es eficiente
E3	Poco eficiente
E4	Poco eficiente.
E5	Ineficiente
E6	Es ineficiente porque el delito sigue en aumento.
E7	Es poco eficiente porque no se logra mayor control de la delincuencia.
E8	Se puede decir que es ineficiente porque la delincuencia sigue en ascenso porque saben que no van ser identificados.
E9	En mi opinión es poco eficiente, porque muy contadas veces se puede identificar a autor del delito.
E10	En mi percepción el desarrollo es eficiente porque existe normas que tipifican la conducta que es muy diferente a su implementación.
E11	Es poco eficiente el desarrollo del sistema penal porque no se puede controlar la delincuencia de suplantación de identidad.
E12	El desarrollo del sistema penal en suplantación de identidad mediante tecnología es un buen refugio de los delincuentes para retirar fácilmente dineros o compras de una caja o banco; por eso creo que es poco eficiente.
E13	El delito de suplantación de identidad por medios tecnológicos sigue en aumento por ello creo que es poco eficiente.
E14	En el entendido que el sistema penal es un conjunto de instituciones como PNP, juzgado, fiscalía, INPE y otros; en eses sentido, puedo afirmar que es ineficiente.
E15	El desarrollo de la suplantación de identidad es poco eficiente debido a que el aparato del Estado no ha podido contralar este delito.
E16	La suplantación de la identidad es una modalidad fácil para los delincuentes cibernéticos para obtener grandes ganancias ilícitas, por lo que considero que es poco eficiente.
E17	El desarrollo en el sistema penal del delito de suplantación de identidad por medios tecnológicos es una amenaza enorme porque sigue en aumento, razón por la cual considero que es ineficiente.
E18	El desarrollo del delito de suplantación de identidad mediante la tecnología, es un gran riesgo para las personas naturales y jurídicas, por eso considero que es poco eficiente.
E19	Es ineficiente porque el sistema penal no ha podido controlar este tipo de delitos.
E20	Considero que es ineficiente porque el delito sigue en acceso y no es posible controlar.

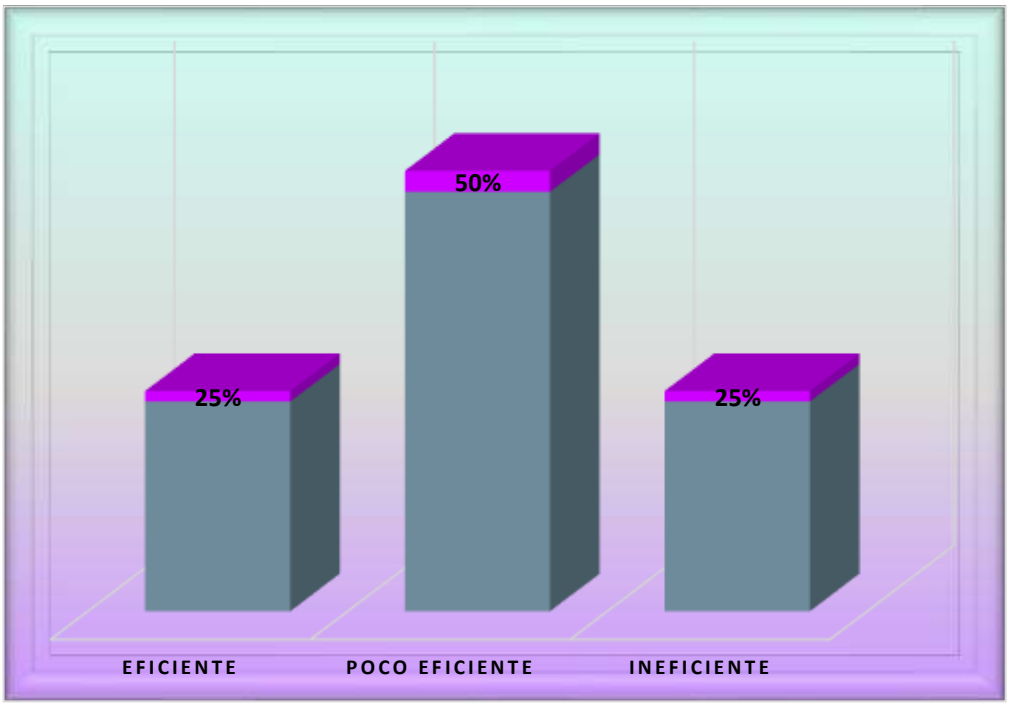
Tabla 23

Resultados de Entrevista número Diez – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	5	25%
Poco eficiente	10	50%
Ineficiente	5	25%
TOTAL	20	100%

Figura 10

Resultados de Entrevista número Diez – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los señores fiscales, se obtuvo como resultado que un 25% de entrevistados indican que es EFICIENTE el desarrollo en el sistema jurídico nacional el delito de suplantación de identidad, el 50% indican que es POCO EFICIENTE y finalmente el 25% indican que es INEFICIENTE.

Tabla 24

Entrevista número Once, realizados a los Fiscales

Nº de entrevistados	Según su opinión ¿El control de los factores de la impunidad en los delitos informáticos en el sistema penal peruano, es eficiente, poco eficiente o ineficiente?
E 1	Es ineficiente en el control de los factores, porque no existe una adecuada capacitación al usuario para manipular dispositivos electrónicos.
E2	Es poco eficiente, porque la falta de capacitación a los efectivos policiales y a los ficales contribuyen al aumento de este tipo de delitos.
E3	Es poco eficiente porque los aparatos logísticos no son los adecuados para perseguir el delito informático.
E4	Es poco eficiente porque la falta de conocimiento de los ciudadanos usuarios de dispositivos electrónicos contribuye en los delitos cibernéticos.
E5	Creo que es poco eficiente porque la falta de implementación a nivel nacional hace que los delitos cibernéticos están en aumento.
E6	Es poco eficiente debido a que en las regiones no están implementados este tipo de delitos informáticos.
E7	Es poco eficiente porque los factores como falta de capacitación en las regiones de los operadores del derecho contribuyen en el aumento de delitos informáticos.
E8	Considero que es poco eficiente porque el desconocimiento de los ciudadanos en el manejo de aplicativos informáticos, conducen a ser víctimas muy fácilmente.
E9	En el control de los factores opino que es poco eficiente porque necesita mucha trabajar en la prevención a fin de evitar ser víctima de delitos cibernéticos.
E10	La implementación de la Ley en ese capítulo del penal se mantiene vigente
E11	Los factores como la falta de seguridad de las entidades hacen que es ineficiente en este aspecto.
E12	Es ineficiente en el control de factores
E13	Para enfrentar el delito informático hay que tener personal especializado y equipos de alta generación, la misma que no existe en nuestra región por lo tanto seria poco eficiente.
E14	Los factores como la falta de implementación con equipos de última generación de parte del estado es ineficiente.
E15	Creo que ante varios factores es poco eficientes.
E16	Es poco eficiente debido a que los factores de implementación en todas las regios es cero.
E17	Los factores como la falta de capacitación a los agentes policiales y fiscales son ineficientes para enfrentar este tipo de delitos.
E18	Es ineficiente el control de los delitos cibernéticos, porque ante la diversidad de factore los ciberdelincuentes están al asecho siempre.
E19	El control de los factores en la comisión de delitos informáticos es poco eficiente.
E20	Los factores son múltiples, por lo que considero que es poco eficiente al no poder controlar.

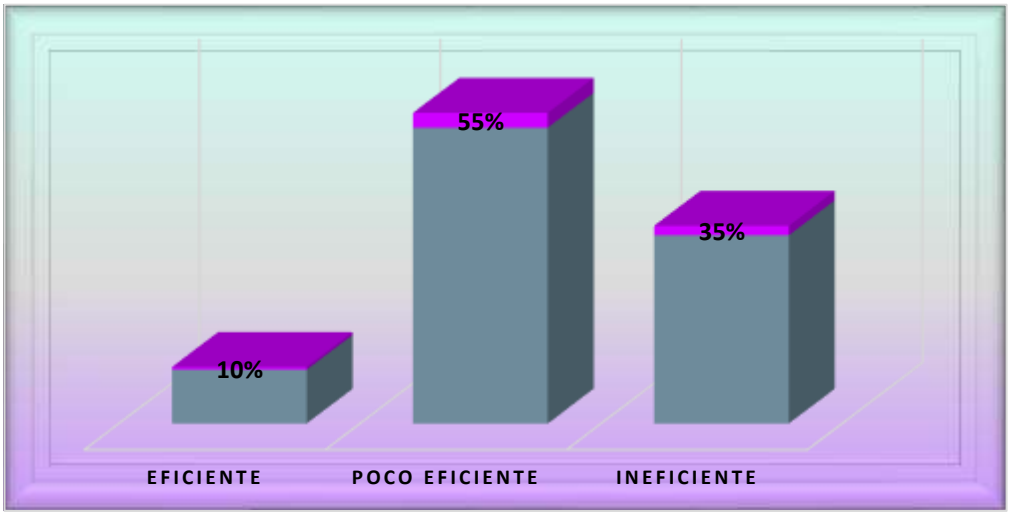
Tabla 15

Resultados de Entrevista número Once – realizados a los Fiscales

ESC. VLT	Fi	%
Eficiente	2	10%
Poco eficiente	11	55%
Ineficiente	7	35%
TOTAL	20	100%

Figura 11

Resultados de Entrevista número Once – realizados a los Fiscales



Interpretación: De las entrevistas realizadas a los señores fiscales, se obtuvo como resultado que solo un 10% de entrevistados indican que es EFICIENTE el control de los factores de la impunidad en los delitos informáticos en el sistema penal peruano, el 55% indican que es POCO EFICIENTE y un 35% de entrevistados indican que es INEFICIENTE.

4.2. Discusión de resultados

En la determinación del desarrollo de los delitos informáticos en el sistema penal peruano tipificados en la Ley especial Nº 30096 modificado por Ley Nº 30171 en los años, 2020 -2022, es entre ineficiente y poco eficiente, debido a que por un lado la legislación tipifica los delitos, pero su aplicación es ineficiente por falta de implementación con personal capacitado y la falta de equipos de última generación que permita identificar a los sujetos activos de los delitos cibernéticos.

Los delitos cibernéticos, son hechos ilícitos que se cometen usando como medio los dispositivos electrónicos, usando computadoras, celulares, redes electrónicas, sistemas informáticos, entre otros artefactos que se viene desarrollando.

El delito informático está en aumento sistemático, conforme se difunde los avances informáticos nace una nueva forma de cometer el delito; es decir, de la

misma forma de la digitalización y el uso de internet aumenta los delitos por este medio.

Los delitos informáticos, se ha ido incorporando paulatinamente, primero se ha introducido a diferentes delitos en el catálogo de delitos del Código Penal de 1991, tales como el numeral 4 del segundo párrafo del artículo 186 y los artículos 207.º-A, 207.º-B, 207.º-C y 207.º-D, Luego se introduce una Ley especial 30096, publicándose el 22 de octubre de 2013 y actualizado mediante Ley Nº32183, publicada el 11 de diciembre de 2024 que incorporó el art. 8.º-A.

En el delito también contribuyese el desconocimiento de los usuarios de un determinado aplicativo, que aprovecha los sujetos para clonar o copiar sus claves; el otro factor es el aumento del uso del internet, los trabajos remotos y el uso frecuente del internet son elementos que contribuye en el aumento de delitos informáticos.

Sin embargo, la percepción de los entrevistados que son especialistas por tener a su cargo la investigación de los delitos informáticos, se resume que un 30 % de nuestra muestra nos indican que es ineficiente el nivel de desarrollo del delito contra el sistema informático en el sistema penal peruano, un 25% nos indican que es poco eficiente pero un buen porcentaje indican que es ineficiente con un 45%; éste último por los resultados de su aplicación de la ley vigente (Figura Nº 3).

Se ha podido establecer que los hechos que afectan bienes jurídicos a personas físicas no están tipificados como delitos informáticos en el sistema penal peruano; debido a que la mayoría de los delitos se cometen en una transacción con los bancos o casi nunca en una transacción entre personas naturales; sin embargo, existe estafas cibernéticas individuales mediate el uso de dispositivos electrónicos.

En el sistema penal es conocidos que el bien jurídico cumple funciones de gran importancia para las ciencias penales; porque “permite fundamentar el

castigo punitivo de las conductas que lo lesionan o ponen en peligro y constituye un requisito ineludible para el ejercicio del *ius puniendi* del Estado*"* Ferrajoli (2012 p. 7), citado por (Mayer, 2017)

En el entendido que el objeto de tutela bienes jurídicos, el derecho protegido, interés jurídicamente tutelado, bien garantizado, objeto jurídico, núcleo del tipo, objeto de protección o simplemente es el interés o la utilidad social; denotan que los bienes necesitados de protección mediante la ley, "con el fin último de garantizar todo tipo de derechos, valores y bienes a partir del reconocimiento esencial de su pertenencia, buen uso y disfrute de cada persona". (Zamora, 2008).

"El reconocimiento de la funcionalidad informática como bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, junto con incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales" (Mayer, 2017). Como una interconexión individual o masiva entre individuos, que es un bien jurídico instrumental.

En abstracto los bienes jurídicos están protegidos debido a que existen figuras legales tipificados en los instrumentos legales; sin embargo, en el plano concreto se convierte en ineficientes porque más de 45% de los entrevistados califican como ineficiente en la protección concreta de bienes jurídicos.

Se ha logrado establecer el incremento de los delitos informáticos en el sistema penal peruano, en las últimas décadas se han incrementado exponencialmente, sin embargo, la aplicación de las normas ha sido ineficientes por factores logísticos de capacitación, entrenamiento de los agentes policiales y fiscales y la falta de tecnología adecuada para rastrear e identificar a los sujetos activos del deleito, que la mayoría quedan en impunes.

El delito informático, seguirá aumentando, porque la tecnología se viene renovando paulatinamente, de modo que, no sorprenderá en el futuro el

surgimiento de otros delitos informáticos; además, teóricamente se encuentra en pleno desarrollo desde el ámbito jurídico.

La era informática, es por los progresos de las computadoras, la capacidad de almacenamiento y procesamiento, la miniaturización de los chips en productos industriales, “la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la” (Pino, s.f.).

El desarrollo de la era informática, es continua o permanente, de modo que el sistema penal viene recogiendo diferentes elementos para proteger el bien jurídico, tipificando los delitos en el sistema penal; la prueba seria las continuas modificaciones que inició el año 2013 con la publicación de la Ley Nº 30096; 2014 se emite la Ley Nº 30171 que modifica el artículo 1; el 2023 D.L. Nº 1571; el 2023 Decreto Ley Nº1614; el año 2024 el Decreto Legislativo Nº 1625 y la Ley Nº 32183; este ritmo seguirá ocurriendo en nuestro sistema penal peruano, a la par con el avance tecnológico y las diferentes modalidades de delitos informáticos que se suscitan mediante el uso de la cibernética.

Las entrevistas hechas a los fiscales, como especialistas en la aplicación de la norma jurídica, se obtuvo como resultado que solo 15% de entrevistadas perciben como eficiente el nivel de desarrollo de los delitos informáticos contra la indemnidad sexual y libertad sexual en el sistema penal peruano, pero un por sentaje considerable de 55% de entrevistados indican que es poco eficiente; así mismo un 30% indican que es ineficiente, con respeto a la protección de bienes jurídicos (figura Nº4).

Se ha podido establecer los factores de la impunidad en los delitos informáticos en el sistema penal peruano, son muchas, los desconocimientos del uso de aplicativos son aprovechados por los facinerosos, la poca seguridad de las entidades bancarias, que fácilmente son quebrantados por los ciberdelincuentes.

El sistema penal peruano opera bajo el principio de legalidad, el cual está constitucionalmente establecido en el artículo 2, inciso 24, literal a): “Nadie está obligado a hacer lo que la ley no manda, ni impedido de hacer lo que ella no prohíbe”. Este principio se complementa con la prohibición de la analogía en el artículo 139, inciso 9: “El principio de inaplicabilidad por analogía de la ley penal y de las normas que restrinjan derechos”. Dichos preceptos garantizan que ninguna persona pueda ser sancionada por hechos que no estén previamente tipificados como delito, asegurando la certeza jurídica y la protección de los derechos fundamentales. Además, refuerzan la idea de que la ley penal debe ser clara, expresa y previa al hecho, limitando la discrecionalidad del Estado y evitando interpretaciones arbitrarias que puedan afectar la libertad de los ciudadanos.

La tipicidad es el eje central del sistema penal peruano; si los elementos del tipo no encuadran en el hecho, este simplemente se considera atípico. En ciencias penales, no es posible interpretar la ley por analogía para perjudicar a un procesado, ya que ello vulneraría el principio de legalidad. Por esta razón, la ley debe ser previa al hecho, expresa y clara, de manera que permita subsumir el hecho concreto al tipo penal correspondiente. La tipicidad garantiza seguridad jurídica y protege los derechos fundamentales de las personas, evitando arbitrariedades en la aplicación de la norma. Asimismo, establece límites precisos a la acción del Estado, asegurando que sólo conductas previamente tipificadas puedan ser sancionadas, lo que fortalece la legitimidad y la confianza en el sistema judicial.

Se ha establecido que los factores de impunidad de los autores de los delitos informáticos incluyen la falta de selección de personal especializado y de capacitación de los operadores jurídicos, así como de los operadores en materia de ciberdelincuencia; la carencia de logística, debido a que el Estado no ha implementado a nivel nacional centros especializados de investigación contra la ciberdelincuencia; y la ausencia de equipos de última generación para rastrear e

identificar a los sujetos que cometen delitos por este medio. Estos vacíos estructurales generan dificultades significativas para la persecución penal efectiva, permitiendo que muchos delitos queden sin sanción y desincentivando la confianza en el sistema judicial.

Los participantes con experiencia permanente tienen la percepción de que el 60% de los entrevistados consideran eficiente el nivel de desarrollo del tratamiento de los delitos informáticos contra la intimidad y el secreto de las comunicaciones en el sistema penal peruano; el 30% lo considera poco eficiente, mientras que un 10% indica que es ineficiente. Esta distribución evidencia que, aunque existe un avance relativo en la atención de estos delitos. Además, resalta la necesidad de fortalecer la formación de los operadores, mejorar la infraestructura tecnológica y promover políticas de cooperación interinstitucional para enfrentar la ciberdelincuencia de manera más integral.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se ha logrado determinar que el desarrollo de los delitos informáticos en el sistema penal peruano tipificados en la Ley Especial Nº 30096 modificado por Ley Nº 30171 en los años, se encuentra en continuo desarrollo a la par con los avances tecnológico continuo, cuyo indicador de este fenómeno jurídico es las modificaciones introducidas desde el año 2013 hasta la actualidad; sin embargo, la percepción es de poco eficiente y de ineficientes en cuanto a su aplicación.
- Se ha logrado establecer que los hechos que afectan bienes jurídicos a personas físicas en los delitos informático se garantizan tanto para las personas en forma individual o colectiva en los delitos informáticos en el sistema penal peruano; en forma abstracta los bienes jurídicos están protegidos por la ley, sin embargo, en su aplicación concreta la protección se convierte en ineficiente debido a que los hechos son archivados por no llegar a la identificación de los delitos.
- Se ha podido establecer que en todos los países el delito informático está en aumento, cada vez más las denuncias se incrementan porque las personas intensifican sus transacciones virtuales o electrónicas, haciendo que los delitos también aumenten; asimismo, existen afectados que no denuncian por desconfianza en la capacidad investigativa de las autoridades.
- Se ha logrado establecer los factores de la impunidad en los delitos informáticos en el sistema penal peruano; es por falta de selección de personal especializado y capacitación; la falta de logística, porque el Estado no ha implementado a nivel nacional centros especializados de investigación contra el ciberdelincuencia y la falta de equipos de última generación para

rastrear e identificar a los sujetos que cometen delitos por este medio; el desconocimiento de los usuarios del uso del sistema.

5.2. Recomendaciones

- Se recomienda que el Estado difunda por diferentes medios de comunicación como prevención las diferentes modalidades que los delitos informáticos se cometen, a fin de que el ciudadano tenga mayor cuidado en sus diferentes transacciones y establecer penas drásticas para aquellos que aprovechando su cargo, alteran, clonas tus contraseñas, especialmente aquellos que laboran en instituciones públicas y privadas.
- Las Universidades que cuentan con la facultad de derecho, implementar cursos sobre los delitos informáticos, a fin de establecer con claridad los bienes jurídicos en cada tipo de delitos informáticos, dado que existen muchos ensayos teóricos que no son convincentes.
- El Estado y gobiernos regionales, difundan planes de prevención de delitos cibernéticos, enseñando a los usuarios de las plataformas que tengan mayor cuidado para aminorar los riesgos que cometen entregados sus datos reservados a personas dudosas que usan plataformas virtuales.
- El Estado implemente con personal especializado y equipos de última generación en todas las regiones del país, a fin de que se logre identificar y sancionar a los que responsables de los delitos informáticos en diferentes modalidades.

REFERENCIAS BIBLIOGRÁFICAS

Albuqueroque, J. (s.f.). Recuperado el 03 de 10 de 2023, de https://www.teseopress.com/palabrasclavefronteras/chapter/identidad/

Andina, A. A. (2022). *Conoce las modalidades más comunes de delitos informáticos y cómo denunciarlos en el Perú.* Andina. Obtenido de https://andina.pe/agencia/noticia-conoce-las-modalidades-mas-comunes-delitos-informaticos-y-como-denunciarlos-el-peru-901507.aspx

Arnal, M. (s.f.). Recuperado el 07 de 02 de 2023, de http://www.elalmanaque.com/lexico/delito.htm

Belcic, I. (02 de 05 de 2020). Obtenido de https://www.avast.com/es-es/c-phishing

Bramont-Arias, L. (1997). *El delito informatico en el Código Penal Peruano.* Pontificia Universidad Católica del Perú. Obtenido de file:///C:/Users/NOVO/Downloads/EL%20DELITO%20INFORMATICO%20EN%20EL%20CODIGO%20PENAL%20PERUANO%20-%20OCR%202.pdf

Cataño, T. L., & Panduro, L. L. (2023). *EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO- UCAYALI, 2022.* Universidad Nacional de Ucayali, Pucallpa. Obtenido de http://repositorio.unu.edu.pe/bitstream/handle/UNU/6320/B5_2023_UNU_DERECHO_2023_T_TERESA-CATANO_ET_AL_V1.pdf?sequence=1&isAllowed=y

Centro de Estadistica de Observatorio y Monitoreo de ciberdelitos - OGDI. (s.f.). Recuperado el 03 de 10 de 2023, de https://ogdi.org/historia-del-cibercrimen

Congreso de la Republica. (17 de 07 de 2000). Obtenido de https://cdn.www.gob.pe/uploads/document/file/356824/NORMA_1887_Ley_27309.pdf?v=1567090257

Congreso de La Republica. (17 de 05 de 2004). Obtenido de https://oig.cepal.org/sites/default/files/2004_per_ley28251.pdf

Congreso de la República. (23 de 09 de 2008). Obtenido de https://www.leyes.congreso.gob.pe/Documentos//2006_2011/ADLP/Normas_Legales/29263-LEY.pdf

Covenio. (23 de 11 de 2001). Recuperado el 03 de 10 de 2023, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Defensoria del Pueblo. (2023). *Ciberdelincuencia en el Perú.* INFORME DEFENSORIAL N° 001-2023-DP/ADHPD, Perú-Defensoria del Pueblo. Obtenido de https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Definiciona.com. (23 de 03 de 2020). Obtenido de https://definiciona.com/informatica/

Egg, E. (1995). *Técnicas de investigación social* (24 ed.). Buenos Aires, Argentina.

Ehrhart, M. (18 de 01 de 2023). Obtenido de https://www.dw.com/es/ciberataques-e-inflaci%C3%B3n-lo-que-m%C3%A1s-preocupa-a-las-empresas/a-64430159

Fonseca, T. L., & Martinez, A. M. (2022). *Los delitos informáticos y la problemática trasnacional: el caso colombiano.* Universidad Católica de Colombia, Bogota - Colombia. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/100243219/Capitulo_5_De_los_delitos_transnacionales-libre.pdf?1679712529=&response-content-disposition=inline%3B+filename%3DLos_delitos_informaticos_y_la_problemati.pdf&Expires=1696727990&Signature=VCZP4jRmKPuJc1NtoFH

Hernandez, R., Fernández, C., & Baptista, P. (2014). *Metodologia de la Investigación.* Mac garw-Hill Education.

Lopez, J. (s.f.). Obtenido de https://economipedia.com/definiciones/operacion-financiera.html

Mayer, L. (2017). El bien jurídico protegido en el delito informático. *SciELO*.

Nacions Unidas- Departamento de Asuntos Economicos y Sociales. (s.f.). Obtenido de https://www.un.org/es/desa/seguridad-cibernetica

Paucar, E. (202). *Metodologia y tesis cazando ideas.* Editores Gamarra.

Paucar, E. (2020). *Metodología y Tesis.* Gamarra Editore.

Peña, A. (2008). *Derecho penal. Parte especial.* IDEMSA.

Peralta, R. (2022). *Los delitos informaticos y los datos en el sistema infromatico.* Tesis para optar titulo de abogado, Universidad Peruana de las Américas. Obtenido de http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/2572/1.Ricardo%20Peralta%20-%20Delitos%20informaticos%20-%2015%20Marzo.pdf?sequence=1&isAllowed=y

Perù. (05 de 09 de 2022). *infobae*. Obtenido de https://www.infobae.com/america/peru/2022/09/05/delitos-informaticos-se-han-incrementado-en-el-peru/

Pino, A. d. (s.f.). Delito Informático. *Profesor de Derecho Informático de la PUCE*. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Puelles, R. (2021). Taller de delitos ciberneticos. *Observatorio Peruano de ciberdelitos del Perú*. Lima. Recuperado el 04 de 10 de 2023, de https://www.youtube.com/watch?v=ceM7FJuny0I

Ramos, J. (2008). *Epistemologia Juridica.* San Marcos.

Sanchis, E. (02 de 01 de 2024). Obtenido de https://peritos-informaticos.com/blog/principales-delitos-informaticos-en-espana/

Villavicencio, F. (2014). Delitos informáticos. Ius et Veritas. *Ius et Veritas*, 24(49), 284-304.

Vinelli, R. (2021). Los delitos informáticos y su relación en la criminalidad económica. *Univercidad de Lima*. doi:doi: https://doi.org/10.26439/iusetpraxis2021.n053.4995

Zamora, A. (2008). Obtenido de https://cuci.udg.mx/sites/default/files/bien_juridico.pdf

ANEXOS

ANEXO 1. MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
Problema General	**Objetivo General**	**Hipótesis General**			**X1.1.** Delito contra el sistema informática. X1.2. Delitos informáticos contra la indemnidad sexual y libertad sexual. X1.3. Delitos informáticos contra la intimidad y secreto de las comunicaciones. X1.4. Delitos informáticos contra el patrimonio. X1.5. Delitos informáticos contra la fe pública. .	• **Sistema de métodos Método general:** Inductivo - deductivo • **Tipo de investigación:** Básica **En el tiempo:** Transversal. **Nivel de la investigación:** Descriptivo **Diseño de la investigación:** No Experimental **Enfoque de la investigación:** cualitativa • **Población y muestra** **Población:** 20 fiscales penales de coronel portillo **Muestra:** 20 • **Técnicas recolección de datos** **Técnicas:** Entrevista **Instrumentos:** Guía de entrevista, **Técnicas de procesamiento de datos:** Se procedió a analizar los datos mediante la herramienta de EXCEL,
¿Cuál es el desarrollo jurídico de los delitos informáticos en el sistema penal peruano en los años, 2020 - 2022?	Determinar el desarrollo jurídico de los delitos informáticos en el sistema penal peruano en los años, 2020 -2022.	El desarrollo jurídico de los delitos informáticos en el sistema penal peruano en los años, 2020 -2022, se encuentra en proceso de constante modificación.	**DELITO INFORMATICO EN EL SISTEMA PENAL PERUANO**	**X1:** Leyes Especiales Nº 30096, modificado por Ley Nº 30171		
				X2: El Código Penal de 1991	X2.1 Hurto telemático, art.186. X2.2. Delito informático Ley Nº 27309. X2.3. Turismo sexual infantil -Ley Nº 28251. X2.4. Clonación o adulteración de terminales de telefonía celular.	

Problemas específicos	Objetivos específicos	Hipótesis especificas	
¿Cuál es el desarrollo jurídico de los delitos informáticos en el sistema general del Código Penal peruano de 1991 en los periodos, 2020 a 2022? ¿Cuál es el desarrollo jurídico de los delitos informáticos mediante leyes especiales Nº 30096 modificado por Ley Nº 30171 en los periodos 2020 a 2021?	Establecer es el desarrollo jurídico de los delitos informáticos en el sistema general del Código Penal peruano de 1991 en el periodo 2020 a 2022. Establecer el desarrollo jurídico de los delitos informáticos mediante leyes especiales Nº 30096 modificado por Ley Nº 30171 en los periodos 2020 a 2021.	El desarrollo jurídico de los delitos informáticos en el sistema general del Código Penal peruano de 1991 en el periodo 2020 a 2022, de modificación y derogación constante. El desarrollo jurídico de los delitos informáticos mediante leyes especiales Nº 30096 modificado por Ley Nº 30171 en los periodos 2020 a 2021, se especializa dejando el sistema ordinario.	X2.5. Apología al terrorismo. D. Lrg. Nº 982. X2.6. Delito de propiedad intelectual, Ley Nº 29263. X2.7. Ingreso y sabotaje a centros de reclusión. Ley 29867

Fuente: *Propia*

ANEXO 2. MATRIZ DE INSTRUMENTOS

VARIABLE DE ESTUDIO	DIMENSIONES	INDICADORES	ÍTEMS
VARIABLE X DELTO INFORMATICO EN EL SISTEMA PENAL PERUANO	**X1:** Leyes Especiales Nº 30096, modificado por Ley Nº 30171	**X1.1.** Delito contra el sistema informática. X1.2. Delitos informáticos contra la indemnidad sexual y libertad sexual. X1.3. Delitos informáticos contra la intimidad y secreto de las comunicaciones. X1.4. Delitos informáticos contra el patrimonio. X1.5. Delitos informáticos contra la fe pública. .	1. ¿Cuál es el nivel de desarrollo del delito contra el sistema informático en el sistema penal peruano? 2. ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la indemnidad sexual y libertad sexual en el sistema penal peruano? 3. ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la intimidad y secreto de las comunicaciones en el sistema penal peruano? 4. ¿Cuál es el nivel de desarrollo de los delitos informáticos contra el patrimonio en el sistema penal peruano? 5. ¿Cuál es el nivel de desarrollo de los delitos informáticos contra la fe pública en el sistema penal peruano?
	X2: El Código Penal de 1991	X2.1 Hurto telemático, art.186. X2.2. Delito informático Ley Nº 27309. X2.3. Turismo sexual infantil -Ley Nº 28251. X2.4. Clonación o adulteración de terminales de telefonía celular. X2.5. Apología al terrorismo. D. Leg. N.º 982. X2.6. Delito de propiedad intelectual, Ley Nº 29263. X2.7. Ingreso y sabotaje a centros de reclusión. Ley 29867	6. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal? 7. ¿Cuál es el desarrollo en el sistema jurídico nacional los delitos informáticos incorporados al Código Penal mediante Ley Nº 27309? 8. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de turismo sexual infantil incorporado al Código Penal mediante Ley Nº 28251? 9. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de clonación o adulteración de terminales de telefonía celular incorporados al Código Penal? 10. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de apología al terrorismo del D. Leg N.º 982? 11. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de propiedad intelectual incorporado al Código Penal mediante Ley Nº 29263? 12. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de ingreso y sabotaje en centros de reclusión incorporados al Código Penal mediante Ley Nº 29867?

Fuente: *propia*

ANEXO 1. FICHA DE OPINION DE EXPERTOS

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

I. DATOS GENERALES

Apellidos y nombres de los autores	**Facultad**
1. SALCEDO PIÑA, KATY ARACELI. 2. GRANADOS PAREDES, JESÚS FELIPE	Derecho y CC. PP -UNU

II. ASPECTOS DE VALIDACIÓN

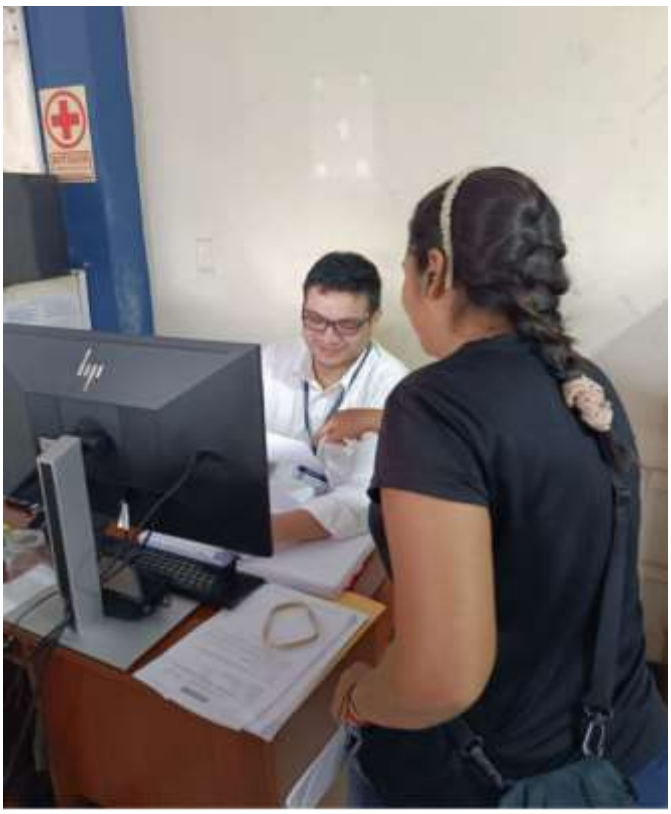
INDICADORES	CRITERIOS	DEFICIENTE **1-20%**	REGULAR **21-40%**	BUENO **41-60%**	MUY BUENO **61-80%**	EXCELENTE **81-100%**	SUGERENCIAS
1.CLARIDAD	Esta formulado con lenguaje apropiado					**X**	
2.OBJETIVIDAD	Esta expresado en situaciones observables					**X**	
3.ACTUALIDAD	Esta de acorde con el avance legislativa				**X**		
4.ORGANIZACIÓN	Existe una organización lógica entre variables e indicadores				**X**		
5.SUFICIENCIA	Comprende los aspectos de contenido jurídico.				**X**		
6.INTENCIONALIDAD	Adecuado para valorar el objeto de estudio sobre desarrollo legislativo					**X**	
7.CONSISTENCIA	Existe una relación de pertinencia, entre problema, objetivo y hipotesis				**X**		
8.COHERENCIA	Existe relación entre indicadores y dimensiones					**X**	
9.METODOLOGIA	Responde al propósito de la investigación.					**X**	

III. OPINION DE APLICABLIDAD: SI

IV. PROMEDIO DE VALORACIÓN :80%

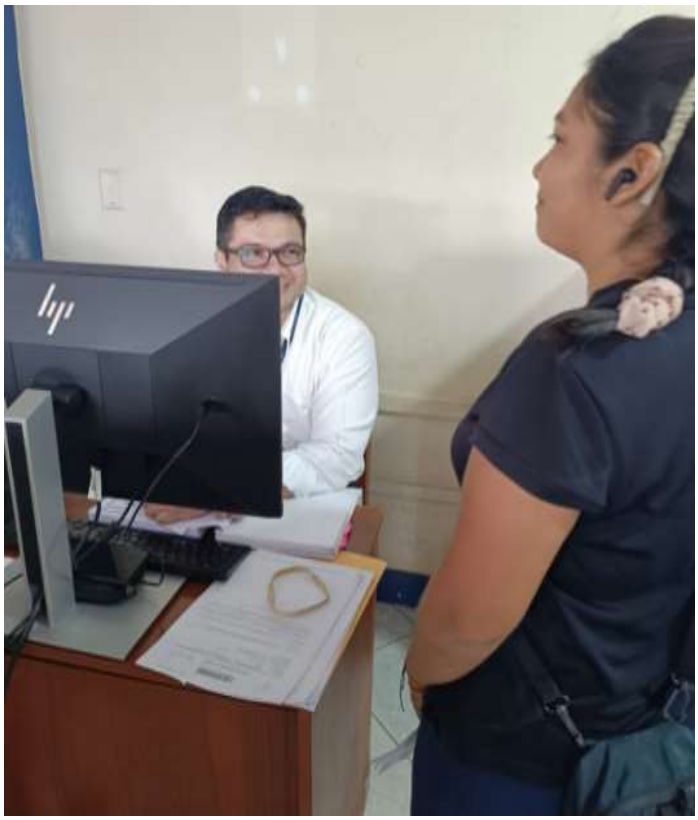
Firma de validador:

ANEXO 4. EVIDENCIAS DURANTE LA ENTREVISTA REALIZADAS













UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLITICAS

GUÍA DE ENTREVISTA

INSTRUCCIONES: Estimados usuarios, estamos realizando una investigación titulada "DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO,2020 -2022" tu respuesta es de suma importancia por ello debe leer de manera detallada y responder

- Tesistas: Bach. KATY ARACELI SALCEDO PIÑA.
  Bach. JESÚS FELIPE GRANADOS PAREDES.

1. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal?
   Este delito se incorporo en el articulo 186 d:l
   ... que decia modalidad mediante la agrupa...
   ... con ... de ... con ... uso ...
   ... la tecnologia de la informacion y la comunicacion
2. ¿Cuál es el desarrollo en el sistema jurídico nacional los delitos informáticos incorporados al Código Penal mediante Ley Nº 27309?
   ... se ha desarrollado de manera progresiva ...
   ... se da en la actualidad de diferentes ...
   ... maneras que se dan con el ...
   ... de la tecnologia
3. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de turismo sexual infantil incorporado al Código Penal mediante Ley Nº 28251?
   .....
   .....
   .....
   .....
4. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de clonación o adulteración de terminales de telefonía celular incorporados al Código Penal?
   Este delito tiene ... en el pais ...
   ... con ... en ... y ... a ...
   ... de ... la ...
   .....
5. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de apología al **terrorismo** del D. Leg. 982?
   .....
   .....
   .....
   .....

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

GUÍA DE ENTREVISTA

INSTRUCCIONES: Estimados usuarios, estamos realizando una investigación titulada **DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO.2023**", tipo básico-teórico, de enfoque cualitativo, de nivel descriptivo y no experimental, tu respuesta es de suma importancia por ello debe leer de manera detallada y responder.

- Tesistas: Bach. KATY ARACELI SALCEDO PIÑA.

  Bach. JESÚS FELIPE GRANADOS PAREDES.

1. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal?

   EL DESARROLLO ES REGULAR, DE PARTE DE TECNICA Y LA OTRA NEGATIVA

2. ¿Cual es el desarrollo en el sistema jurídico nacional los delitos informáticos incorporados al Código Penal mediante Ley N° 27309?

   ES MUY BAJO EL NIVEL EN GENERAL, POR ANIVEL NACIONAL PUES ESTE DELITO CON OTROS DATOS

3. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de turismo sexual infantil incorporado al Código Penal mediante Ley N° 28251?

   EN HUANUCO ES MUY BAJO, A NIVEL NACIONAL SI DESDE NUESTRA PERSPECTIVA PROCESAL

4. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de clonación o adulteración de terminales de telefonía celular incorporados al Código Penal?

   EL DELITO ES BAJO, POCO PARA CONOCIMIENTO ESTE DELITO PUEDE RECABARSE DATOS ESTADISTICOS PENALES

5. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de apología al terrorismo del D. Leg? 982?

   ESPECIFICAMENTE AL TERRORISMO, SU DESARROLLO ES REGULAR YA QUE SE ENCUENTRA DENTRO DEL CODIGO DE CONCLUSIONES QUE LOS ARTS. 90,

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLITICAS

GUÍA DE ENTREVISTA

INSTRUCCIONES: Estimados usuarios, estamos realizando una investigación titulada "DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO,2020 -2022" tu respuesta es de suma importancia por ello debe leer de manera detallada y responder.

- Tesistas: Bach. KATY ARACELI SALCEDO PIÑA.
  Bach. JESÚS FELIPE GRANADOS PAREDES.

1. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal?
   EL HURTO TELEMÁTICO SON DELITOS INFORMÁTICOS EN NUESTRO SISTEMA LOS CUALES LOS DELINCUENTES A QUE LOS BANCOS SOCIALES Y PRIVADOS HAN TENIDO QUE COMPARSE A NUEVAS TECNOLOGÍAS DE INVESTIGACIÓN.
2. ¿Cuál es el desarrollo en el sistema jurídico nacional los delitos informáticos incorporados al Código Penal mediante Ley Nº 27309?
   ESTA LEY INCORPORO UN CONJUNTO DE DISPOSICIONES PARA TIPIFICAR Y SANCIONAR LOS DELITOS INFORMÁTICOS EN RESPUESTA AL CRECIENTE USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA NECESIDAD DE ABORDAR LOS DESAFÍOS LEGALES DE LA CIBERDELINCUENCIA.
3. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de turismo sexual infantil incorporado al Código Penal mediante Ley Nº 28251?
   LA INCORPORACIÓN DEL DELITO DE TURISMO SEXUAL INFANTIL EN EL CÓDIGO PENAL PERUANO REFLEJA UNA RESPUESTA LEGAL A LA GRAVE PREOCUPACIÓN POR LA EXPLOTACIÓN SEXUAL DE NIÑOS, NIÑAS Y ADOLESCENTES EN EL CONTEXTO DEL TURISMO.
4. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de clonación o adulteración de terminales de telefonía celular incorporados al Código Penal?
   EL DESARROLLO LEGISLATIVO DEL DELITO DE CLONACIÓN DE TELÉFONOS MÓVILES HA PRESENTADO UNA RESPUESTA JURÍDICA PARA LOS DELINCUENTES INFORMÁTICOS PARA LOS FUTUROS DELINCUENTES QUE PUEDAN COMETER ESTE DELITO.

5. **¿Cuál es el desarrollo en el sistema jurídico nacional el delito de apología al terrorismo del D. Leg. 982?**
   CONSISTE QUE LA APOLOGÍA DEL TERRORISMO EN EL PERÚ ES UN DELITO QUE CONSISTE EN LA EXALTACIÓN, PROMOCIÓN O JUSTIFICACIÓN DE ACTOS TERRORISTAS O PERSONAS QUE COMETEN LA COMISIÓN PÚBLICA DE ELLOS, OPINIONES O CONDUCTAS.

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLITICAS

GUÍA DE ENTREVISTA

INSTRUCCIONES: Estimados usuarios, estamos realizando una investigación titulada "DESARROLLO DE LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL PERUANO,2020 -2022" tu respuesta es de suma importancia por ello debe leer de manera detallada y responder .

- Tesistas: Bach. KATY ARACELI SALCEDO PIÑA.
  Bach. JESÚS FELIPE GRANADOS PAREDES.

1. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de hurto telemático que fue tipificado en el art. 186 del Código Penal?
   El hurto telemático, tipificado en el artículo 186 del C P ha evolucionado en su desarrollo dentro del sistema jurídico nacional especialmente a raíz de la creciente incidencia del delito informático.
2. ¿Cuál es el desarrollo en el sistema jurídico nacional los delitos informáticos incorporados al Código Penal mediante Ley Nº 27309?
   La ley 27309 marca un hito significativo en el sistema jurídico peruano al incorporar los delitos informáticos al C P, esta ley responde a la necesidad de adaptar la legislación nacional a los avances tecnológicos y a la creciente incidencia de delitos relacionados con el uso de sistemas informáticos
3. ¿Cuál es el desarrollo en el sistema jurídico nacional del delito de turismo sexual infantil incorporado al Código Penal mediante Ley Nº 28251?
   Esta ley 28251 tuvo importancia significativa para el desarrollo del delito de turismo sexual infantil ya que aborda de manera específica los delitos relacionados a estos. esta ley introduzco el Art. 181-A que establece penas para quienes promuevan, auspicien y faciliten este tipo de explotación
4. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de clonación o adulteración de terminales de telefonía celular incorporados al Código Penal?
   En cuanto a su desarrollo sobre este delito ha experimentado importantes modificaciones, particularmente a través del Art. 222-A del C P. este artículo ha sido objeto de reformas que buscan fortalecer la lucha contra el uso ilegal de dispositivos moviles, en consecuencia combatir la criminalidad asociada a estos delitos.
5. ¿Cuál es el desarrollo en el sistema jurídico nacional el delito de apología al terrorismo del D. Leg. 982?
   su desarrollo a evolucionado a pasos acelerados segun el DL 982 este decreto, estableció las bases para la tipificación de la apología al terrorismo, ha sido objeto de reformas y analisis en el contexto de la legislación peruana ya que refleja un esfuerzo por equilibrar la seguridad nacional con los derechos humanos y sus penas al quebrantamiento de estos como el delito de apología al terrorismo.