UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

CIBERDELINCUENCIA Y DELITOS INFORMÁTICOS EN LA PROVINCIA DE CORONEL PORTILLO AÑO 2023

Tesis por optar el título profesional de

ABOGADO

FRANCISCO EDUARDO RENGIFO SILVA

Pucallpa, Perú

2025

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ACTA DE EXAMEN PARA OPTAR EL TITULO DE ABOGADO

En la ciudad de Pucallpa, siendo las 1:00 Pm del día viernes 07 de febrero del año 2025, 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 "CIBERDELINCUENCIA Y DELITOS INFORMATICOS EN LA PROVINCIA DE CORONEL PORTILLO AÑO 2023", presentado por el bachiller en Derecho y Ciencias Políticas: **FRANCISCO EDUARDO RENGIFO SILVA.**
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. LIZANDRO LEVEAU PEZO (Miembro) y Dr. WASHINGTON TARCICIO QUINTANILLA OSORIO (Miembro), designados con Memorando Múltiple Nº 024/2025-UNU/FDyCP/GyT de fecha 04 de febrero del 2025; luego del cual el señor presidente instó al Secretario Académico a presentar al bachiller examinado.

Acto seguido el Presidente del Jurado invitó al bachiller 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 satisfactoria por el ponente.

Continuando con el desarrollo de la sustentación y de conformidad con el Reglamento de Grados y Títulos, el presidente invitó al bachiller examinado 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 el bachiller: **FRANCISCO EDUARDO RENGIFO SILVA** fue APROBADO POR UNANIMIDAD CON MENCION SOBRESALIENTE.

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 2:00 Pm. Del mismo día, lo suscribieron en señal de conformidad; de lo que doy fe.

Dr. JUAN ARQUIMEDES NUÑEZ TERREROS
PRESIDENTE

Dr. LIZANDRO LEVEAU PEZO
MIEMBRO

Dr. WASHINGTON TARCICIO 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. Lizandro Leveau Pezo

Miembro

Dr. Washington Tarcicio Quintanilla Osorio

Miembro

Dr. Joel Orlando Santillán Tuesta

Asesor

Bach. Francisco Eduardo Rengifo Silva

Tesista

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº **V/0633-2024** .

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

"**CIBERDELINCUENCIA Y DELITOS INFORMÁTICOS EN LA PROVINCIA DE CORONEL PORTILLO AÑO 2023**"

Autor(es)	:	**RENGIFO SILVA, FRANCISCO EDUARDO**
Facultad	:	**DERECHO Y CIENCIAS POLÍTICAS**
Escuela	:	**DERECHO**
Asesor(a)	:	**Dr. SANTILLAN TUESTA, JOEL ORLANDO**

Presenta un **porcentaje de similitud de 5%,** 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: 08/11/2024

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, Francisco Eduardo Rengifo Silva

Autor de la tesis titulada : Ciberdelincuencia y delitos Informáticos en la provincia de Coronel Portillo año 2023

Sustentada el año 2025

Asesor(a): Dr. Joel Orlando Santillan Tuesta

Facultad: Derecho y Ciencias 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: 07/02/2025

Email: ferspucallpa@hotmail.com Firma:

Teléfono: 947893149 DNI: 41541069

DEDICATORIA

A Dios, por brindarme la vida, la salud y la fortaleza necesarias para completar este trabajo, y por guiar mis pasos en cada momento.

A mis padres, por su amor incondicional, su apoyo constante y por enseñarme el valor del esfuerzo y la perseverancia. Su confianza en mí ha sido una fuente inagotable de motivación.

A cada uno de mis docentes, quienes, con su sabiduría y dedicación, han dejado una huella imborrable en mi formación académica y personal. Gracias por su paciencia, su entrega y por inspirarme a seguir adelante.

AGRADECIMIENTO

A la Universidad Nacional de Ucayali, por proporcionarme los recursos y las oportunidades necesarias para recibir una educación de calidad y por las demandas académicas que me han preparado para el ámbito profesional.

A los docentes, cuyas vastas sabiduría y dedicación han sido fundamentales en mi formación académica y personal.

A mi familia, por su constante apoyo y confianza a lo largo de todos estos años.

A mi asesor, Dr. Orlando Santillán Tuesta, cuya guía y consejos han sido indispensables para la realización de esta investigación.

ÍNDICE GENERAL

Pág.

DEDICATORIA vi

AGRADECIMIENTO vii

ÍNDICE GENERAL viii

ÍNDICE DE TABLAS x

ÍNDICE DE FIGURAS xi

RESUMEN xii

ABSTRACT xiii

INTRODUCCIÓN xiii

CAPÍTULO I. EL PROBLEMA DE INVESTIGACIÓN 1

1.1. Descripción del problema 1

1.2. Formulación de problema 4

1.2.1. Problema general 4

1.2.2. Problemas específicos 4

1.3. Objetivo general y objetivos específicos. 5

1.3.1. Objetivo general 5

1.3.2. Objetivos específicos 5

1.4. Justificación. 5

1.5. Delimitación 7

1.6. Viabilidad 11

CAPÍTULO II. MARCO TEÓRICO 15

2.1. Antecedentes de la investigación 15

2.1.1. Antecedentes internacionales 15

2.1.2. Antecedentes nacionales 17

2.1.3. Antecedentes locales 20
2.2. Bases teóricas 21
2.3. Definición de términos básicos 42
2.4. Formulación de hipótesis 45
2.4.1. Hipótesis general 45
2.4.2. Hipótesis específicas 46
2.5. Variables 46
2.5.1. Variable 1 46
2.5.2. Variable 2 46
2.5.3. Operacionalización de las variables 46
CAPÍTULO III. METODOLOGÍA 48
3.1. Diseño de la investigación 48
3.2. Población y muestra 49
3.3. Técnicas e instrumentos de recolección de datos 50
3.4. Técnicas para el procesamiento de la información 51
CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 53
4.1. Resultados 53
4.2. Prueba de hipótesis 69
4.3. Discusión de resultados 69
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 93
5.1. Conclusiones 93
5.2. Recomendaciones 95
REFERENCIAS BIBLIOGRÁFICAS 97
ANEXOS 101

ÍNDICE DE TABLAS

Pág.

Tabla 1. Operacionalización de las variables 47

Tabla 2. Dimensión Delitos computacionales 53

Tabla 3. Dimensión Tasa de incidencia de delitos informáticos 54

Tabla 4. Dimensión Índice de seguridad cibernética 55

Tabla 5. Variable Ciberdelincuencia 57

Tabla 6. Dimensión Hurto informático 58

Tabla 7. Dimensión Fraude informático 59

Tabla 8. Dimensión Estafa informática 60

Tabla 9. Dimensión Sabotaje informático 61

Tabla 10. Variable Delitos informáticos 63

Tabla 11. Existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023 64

Tabla 12. Existe relación entre el panorama actual de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023 65

Tabla 13. Existe relación entre los factores socioeconómicos, tecnológicos y culturales con la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023 66

Tabla 14. Existe relación entre en la seguridad pública en relación a la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023 67

Tabla 15. Existe relación entre el aumento de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023 68

ÍNDICE DE FIGURAS

Pág.

Figura 1. Esquema de la investigación 48

Figura 2. Dimensión Delitos computacionales 53

Figura 3. Dimensión Tasa de indicencia de delitos informáticos..... 54

Figura 4. Dimensión Índice de seguridad cibernética 56

Figura 5. Variable Ciberdelincuencia 57

Figura 6. Dimensiónes Hurto informático..... 58

Figura 7. Dimensión Fraude informático 59

Figura 8. Dimensión Estafa informática 60

Figura 9. Dimensión Sabotaje informático 62

Figura 10. Variable Delitos informáticos..... 63

RESUMEN

La presente investigación se basó esencialmente en determinar la relación entre la cibercriminalidad y su incidencia en la responsabilidad penal de las empresas privadas en la provincia de Coronel Portillo en el año 2023. Esta investigación se realizó en el contexto del creciente aumento de delitos informáticos en el Perú, destacando que dentro de su marco teórico se argumentan mejor las diferentes posiciones doctrinales que tienen los distintos autores sobre la ciberseguridad y las medidas de reparación aplicables. La cibercriminalidad se ha consolidado como una de las amenazas más importantes para las empresas y la sociedad en general, debido a sus graves consecuencias, que incluyen la violación de datos personales, pérdidas económicas significativas, y efectos adversos sobre la confianza y la seguridad digital. Es importante destacar que los delitos informáticos son distintos de los delitos tradicionales, por lo cual, en ciertas circunstancias, una conducta puede ocasionar tanto daños a la infraestructura digital como perjuicios económicos y personales a particulares. La reparación de los elementos afectados por delitos informáticos beneficia a toda la comunidad digital, mientras que la reparación de los daños a particulares se aborda a través de la responsabilidad penal y civil, teniendo en cuenta tanto el daño como el perjuicio (lucro cesante). El objetivo del presente estudio es establecer si realmente existe una correcta aplicación de las normativas penales y civiles en el ámbito de la cibercriminalidad. Para ello, se empleó una muestra de cien personas con el fin de determinar la mejor solución posible a los problemas relacionados con los delitos informáticos.

Palabras clave: Cibercriminalidad, Responsabilidad penal, Delitos informáticos.

ABSTRACT

This research was essentially based on determining the relationship between cybercrime and its impact on the criminal liability of private companies in the province of Coronel Portillo in the year 2023. This research was carried out in the context of the growing increase in computer crimes in the Peru, highlighting that within its theoretical framework the different doctrinal positions that the different authors have on cybersecurity and the applicable reparation measures are better argued. It is considered that these behaviors are contrary to the requirements of the legal system, framed both in criminal terms and in administrative sanctions. Cybercrime has established itself as one of the most important threats to companies and society in general, due to its serious consequences, which include the breach of personal data, significant economic losses, and adverse effects on trust and digital security. It is important to highlight that computer crimes are different from traditional crimes, which is why, in certain circumstances, conduct can cause both damage to the digital infrastructure and economic and personal harm to individuals. The repair of elements affected by computer crimes benefits the entire digital community, while the repair of damages to individuals is addressed through criminal and civil liability, taking into account both the damage and the loss (lost profits). The objective of this study is to establish whether there really is a correct application of criminal and civil regulations in the field of cybercrime. To do this, a sample of one hundred people was used in order to determine the best possible solution to the problems related to computer crimes.

Keywords: Cybercrime, Criminal liability, Computer crimes.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

La ciberdelincuencia y los delitos informáticos representan una realidad contemporánea que ha transformado la forma en que la sociedad interactúa y opera en el mundo digital. En el contexto específico de la provincia de Coronel Portillo en el año 2023, estas formas de delincuencia adquieren un significado particular debido a la intersección de factores socioeconómicos, tecnológicos y culturales que caracterizan a esta región de Perú.

Coronel Portillo, ubicada en la región Ucayali, se enfrenta a desafíos complejos en materia de ciberseguridad. En un mundo cada vez más interconectado, la provincia no está exenta de las amenazas que emergen en el ciberespacio. Durante el año 2023, Coronel Portillo experimentó un aumento en la incidencia de ciberdelitos, que abarcan desde ataques de phishing y fraudes en línea hasta intrusiones en sistemas de infraestructura crítica.

Uno de los principales problemas que enfrentó la provincia fue el crecimiento de los ataques de phishing, una técnica empleada por ciberdelincuentes para obtener información confidencial de manera fraudulenta. Los habitantes de Coronel Portillo se vieron expuestos a correos electrónicos maliciosos que buscaban engañarlos para revelar datos personales o financieros. Esta forma de ciberdelincuencia no solo impactó en la economía local, sino que también erosionó la confianza de

la población en las transacciones en línea y planteó preocupaciones sobre la privacidad y la seguridad de los datos.

Además del phishing, la provincia experimentó un aumento en los casos de Ransomware, una forma de ataque en la que los delincuentes cifran los datos de las víctimas y exigen un rescate a cambio de su liberación. Estos ataques afectaron a empresas locales, instituciones gubernamentales y usuarios individuales, causando interrupciones en los servicios y pérdidas financieras significativas. La falta de preparación y medidas de seguridad adecuadas exacerbó el impacto de estos incidentes en la comunidad, evidenciando la necesidad de una mayor conciencia y preparación en materia de ciberseguridad.

Otro aspecto preocupante fue la proliferación de actividades delictivas en la dark web, una parte de Internet a la que se accede mediante software especializado que garantiza el anonimato. En Coronel Portillo se identificaron casos de tráfico de drogas, armas y datos personales en plataformas de la dark web, lo que planteó desafíos adicionales para las autoridades locales en la prevención y persecución de este tipo de actividades ilegales. La presencia de estos mercados clandestinos en línea refleja la complejidad de la ciberdelincuencia y la necesidad de una respuesta integral por parte de las autoridades.

Además de los delitos financieros y de extorsión, la ciberdelincuencia en Coronel Portillo también tuvo un impacto en la seguridad nacional y la infraestructura crítica. Se reportaron intentos de intrusiones en sistemas de energía, comunicaciones y servicios públicos, lo que puso de relieve la vulnerabilidad de estas redes ante ataques

cibernéticos. Si bien muchos de estos intentos fueron frustrados por medidas de seguridad robustas, la amenaza persistente resaltó la necesidad de una mayor inversión en ciberdefensa y vigilancia.

Además, se plantea iniciativas para mejorar la cooperación entre el sector público y privado en la protección de infraestructuras críticas y la prevención de ataques cibernéticos La adopción de mejores prácticas de seguridad cibernética en empresas y organizaciones, así como la implementación de tecnologías avanzadas de detección y respuesta ante amenazas.

La capacitación y el fortalecimiento de las capacidades de las fuerzas del orden también fueron prioritarios en la lucha contra la ciberdelincuencia. Se desarrollaron programas de formación especializada para policías y agentes de seguridad, con el fin de mejorar su capacidad para investigar y responder eficazmente a los delitos informáticos, así como para recopilar pruebas digitales que puedan utilizarse en los procesos judiciales.

Se hará hincapié en la importancia de la prevención y la concienciación en la lucha contra la ciberdelincuencia. Se promoverá la adopción de prácticas de seguridad cibernética, como el uso de contraseñas seguras, la autenticación de dos factores y la actualización regular del software, entre otros.

La ciberdelincuencia y los delitos informáticos representan un desafío significativo para la provincia de Coronel Portillo en el año 2023, con impactos en la economía, la seguridad pública y la infraestructura crítica. Sin embargo, mediante la implementación de medidas proactivas y

la cooperación entre diferentes actores, se planea avanzar en la prevención y el combate de estas actividades delictivas en el ámbito digital. A medida que la tecnología continúe evolucionando, será fundamental mantener la vigilancia y la adaptación constante para protegerse contra las amenazas emergentes en el ciberespacio.

1.2. Formulación de problema

1.2.1. Problema general

- ¿Cómo se relaciona la ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023?

1.2.2. Problemas específicos

- ¿Cómo se relaciona el marco legal con los delitos informáticos en la provincia de Coronel Portillo 2023?
- ¿Cómo se relacionan las tipologías de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023?
- ¿Cómo se relaciona la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023?
- ¿Cómo se relaciona el incremento de la ciberdelincuencia con delitos informáticos en la provincia de Coronel Portillo 2023?

1.3. Objetivo general y objetivos específicos

1.3.1. Objetivo general

- Determinar qué relación existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

1.3.2. Objetivos específicos

- Determinar cómo se relaciona el marco legal con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Analizar cómo se relacionan las tipologías de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Determinar cómo se relaciona la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Analizar cómo se relaciona el incremento de la ciberdelincuencia con delitos informáticos en la provincia de Coronel Portillo 2023.

1.4. Justificación

La investigación de este tema es crucial debido al impacto significativo que la ciberdelincuencia puede tener en diversos aspectos de la sociedad, incluida la economía, la seguridad pública y la privacidad de los ciudadanos.

En el contexto de Coronel Portillo en el año 2023, la ciberdelincuencia representa una amenaza creciente que requiere una

comprensión profunda y una respuesta adecuada por parte de las autoridades locales, así como de otros actores relevantes en la comunidad. El estudio de este fenómeno proporciona una visión detallada de la naturaleza y el alcance de los delitos informáticos en la provincia, lo que puede servir como base para el desarrollo de estrategias efectivas de prevención y mitigación.

Además, la investigación sobre la ciberdelincuencia en Coronel Portillo en el año 2023 contribuye al avance del conocimiento en el campo de la ciberseguridad y la criminología digital. A través del análisis de casos específicos, tendencias y patrones de comportamiento delictivo, los investigadores pueden identificar factores subyacentes, vulnerabilidades del sistema y posibles soluciones para abordar este problema emergente.

El estudio de la ciberdelincuencia en Coronel Portillo en el año 2023 tiene implicaciones prácticas importantes para la formulación de políticas públicas y la toma de decisiones en materia de seguridad cibernética a nivel local, regional y nacional. Los hallazgos y recomendaciones derivados de la investigación pueden informar el diseño de programas de capacitación, campañas de sensibilización y la asignación de recursos para combatir eficazmente los delitos informáticos.

La ciberdelincuencia en Coronel Portillo en el año 2023 contribuye a la comprensión general de los desafíos y riesgos asociados con la creciente digitalización de la sociedad. A medida que la tecnología continúa evolucionando y desempeñando un papel cada vez más central en la vida cotidiana, es fundamental analizar críticamente las implicaciones de esta

transformación para la seguridad y el bienestar de las comunidades locales.

La investigación sobre la ciberdelincuencia y los delitos informáticos en la provincia de Coronel Portillo en el año 2023 es esencial tanto desde un punto de vista académico como práctico. Proporciona información valiosa sobre un fenómeno complejo y en evolución, y ofrece orientación para abordar los desafíos relacionados con la seguridad cibernética en el contexto específico de esta comunidad. Además, contribuye al avance del conocimiento en el campo de la ciberseguridad y ofrece ideas importantes para la formulación de políticas públicas y la toma de decisiones en esta área crítica.

1.5. Delimitación

1.5.1. Delimitación espacial

La delimitación geográfica se justifica por la necesidad de examinar de manera detallada los casos de ciberdelincuencia y delitos informáticos ocurridos en esta jurisdicción durante el año 2023 y su posible relación con la infraestructura tecnológica y la actividad delictiva en línea.

La elección de la Primera Fiscalía Provincial Penal Corporativa de Coronel Portillo como el ámbito de estudio se basa en su relevancia como institución encargada de investigar y perseguir los delitos informáticos en esta área específica. Además, esta delimitación permite obtener acceso directo a los expedientes judiciales, estadísticas y otros datos relevantes para llevar a cabo un análisis exhaustivo de los casos de ciberdelincuencia y delitos informáticos.

La provincia de Coronel Portillo presenta características sociodemográficas y culturales particulares que pueden influir en la dinámica de la ciberdelincuencia y los delitos informáticos. Por lo tanto, la delimitación espacial se enfoca en comprender cómo estas variables contextuales pueden interactuar con la presencia de actividades delictivas en línea, contribuyendo así a una comprensión más completa de este fenómeno en este contexto específico.

Permite concentrar los esfuerzos de investigación en un área geográfica concreta, lo que facilita la recolección de datos relevantes y la realización de análisis detallados sobre los patrones y tendencias de la ciberdelincuencia. Además, proporciona una base sólida para la formulación de recomendaciones y estrategias de intervención dirigidas a prevenir y abordar los delitos informáticos en la provincia de Coronel Portillo.

1.5.2. Delimitación teórica

Se enfoca en la ciberdelincuencia como objeto de estudio, centrándose específicamente en los casos en los que se evidencia una presunta conexión entre la comisión del delito y el uso de tecnologías informáticas o la manipulación de datos digitales. Este enfoque permite explorar las posibles influencias de los avances tecnológicos, el acceso ilegal a sistemas informáticos o el uso indebido de información digital en la perpetración de delitos informáticos.

Además, la delimitación teórica considera el marco legal y conceptual relacionado con la ciberdelincuencia en el contexto ecuatoriano, incluyendo la definición legal de los delitos informáticos, las

circunstancias agravantes y las respuestas legales ante este tipo de crímenes. Esto proporciona un fundamento sólido para el análisis de los casos específicos dentro de la jurisdicción de la Primera Fiscalía Provincial Penal Corporativa de Coronel Portillo en el año 2023.

El estudio también se apoya en teorías criminológicas y tecnológicas relevantes que abordan la relación entre el uso indebido de la tecnología y la comisión de delitos informáticos, incluyendo el papel de los factores individuales, sociales y contextuales en la génesis de la ciberdelincuencia.

La importancia de considerar el contexto tecnológico y las dinámicas de la era digital en la comprensión de la ciberdelincuencia, destacando la necesidad de examinar las normas, valores y prácticas que pueden contribuir a la perpetuación de los delitos informáticos en la provincia de Coronel Portillo.

Establece los límites y fundamentos conceptuales necesarios para investigar de manera rigurosa y significativa la relación entre la ciberdelincuencia y los delitos informáticos en la mencionada jurisdicción durante el año 2023. Esto implica un análisis detallado de los casos de delitos informáticos ocurridos en Coronel Portillo.

1.5.3. Delimitación temporal

La delimitación temporal del estudio académico sobre Ciberdelincuencia y Delitos Informáticos en la Primera Fiscalía Provincial Penal Corporativa de Coronel Portillo en el año 2023 se enfoca específicamente en analizar los casos de ciberdelincuencia y delitos

informáticos ocurridos durante ese año en dicha jurisdicción. Este enfoque temporal permite una investigación detallada y actualizada sobre el fenómeno de la ciberdelincuencia en una zona geográfica y período de tiempo específicos.

El año 2023 se selecciona como período de estudio debido a su relevancia para comprender la dinámica reciente de los casos de ciberdelincuencia en Coronel Portillo. Analizar los eventos de un año particular proporciona una instantánea precisa de la situación en ese momento, permitiendo identificar patrones, tendencias y posibles factores contribuyentes al fenómeno de los delitos informáticos.

Facilita la recopilación y análisis de datos, así como la identificación de casos específicos para su estudio detallado. Esto garantiza la viabilidad y la profundidad del análisis, ya que el estudio puede centrarse en una muestra representativa de casos de ciberdelincuencia ocurridos durante un período relativamente corto de tiempo.

Al delimitar el estudio al año 2023, se puede también evaluar la efectividad de las respuestas institucionales y legales ante los casos de ciberdelincuencia en ese período específico. Esto incluye examinar la aplicación de la legislación pertinente, la eficacia de las medidas preventivas y la calidad de la atención a las víctimas y sus familias en el ámbito de los delitos informáticos.

Proporciona un marco preciso y relevante para investigar el fenómeno de la ciberdelincuencia y los delitos informáticos en la Primera Fiscalía Provincial Penal Corporativa de Coronel Portillo. Permite un análisis exhaustivo de los casos ocurridos durante ese período y ofrece

descubrimientos significativos para la prevención y persecución del delito en esa localidad en el ámbito de la ciberseguridad.

1.6. Viabilidad

1.6.1. Viabilidad técnica

La viabilidad técnica del estudio sobre ciberdelincuencia y delitos informáticos en el año 2023 es alta debido a varios factores clave. La tecnología necesaria para recopilar y analizar datos relacionados con la ciberdelincuencia está ampliamente disponible y en constante evolución. Con herramientas avanzadas de análisis de datos y software forense, los investigadores pueden examinar patrones, identificar vulnerabilidades y rastrear actividades delictivas en línea con mayor precisión que nunca.

El aumento del acceso a Internet y la creciente dependencia de la tecnología digital han ampliado el alcance y la complejidad de la ciberdelincuencia, lo que proporciona una amplia base de datos potencial para el estudio. La proliferación de dispositivos conectados a Internet, desde teléfonos inteligentes hasta dispositivos domésticos inteligentes, brinda una gran cantidad de datos que pueden ser analizados para identificar tendencias y comportamientos delictivos

La cooperación entre agencias gubernamentales, instituciones académicas y empresas privadas también contribuye a la viabilidad técnica del estudio. El intercambio de información y recursos entre estas entidades permite una comprensión más completa de la ciberdelincuencia y facilita la colaboración en la investigación y prevención de delitos.

Además, el año 2023 ofrece una oportunidad única para investigar la ciberdelincuencia en tiempo real y adaptarse a las tendencias emergentes. Al estar actualizados con las últimas tecnologías y prácticas delictivas, los investigadores pueden desarrollar estrategias más efectivas para combatir la ciberdelincuencia y proteger la seguridad digital.

La viabilidad técnica del estudio de la ciberdelincuencia y delitos informáticos en el año 2023 es alta gracias a la disponibilidad de tecnología avanzada, el acceso a una amplia gama de datos y la colaboración entre diversas entidades. Estas condiciones proporcionan una base sólida para realizar investigaciones exhaustivas y desarrollar soluciones efectivas para abordar este creciente desafío en la era digital.

1.6.2. Viabilidad Social

El estudio de la ciberdelincuencia y los delitos informáticos en el año 2023 es de vital importancia debido a su relevancia en la sociedad contemporánea. En un mundo cada vez más digitalizado, donde la tecnología juega un papel central en la vida cotidiana, comprender y abordar los riesgos asociados con la seguridad informática es fundamental para la protección de los ciudadanos y la estabilidad de las instituciones.

Investigar la ciberdelincuencia en 2023 permitirá identificar nuevas tendencias, amenazas emergentes y patrones de comportamiento de los ciberdelincuentes. Esta comprensión es esencial para desarrollar estrategias efectivas de prevención, detección y respuesta a los ataques cibernéticos.

El estudio de la ciberdelincuencia en 2023 contribuirá a la sensibilización pública sobre los riesgos de seguridad en línea y promoverá una mayor educación en materia de ciberseguridad. Esto ayudará a empoderar a los individuos y organizaciones para proteger sus datos y sistemas contra posibles ataques.

Investigar la ciberdelincuencia y los delitos informáticos en el año 2023 no solo es viable socialmente, sino también esencial para garantizar la seguridad y protección en el entorno digital en constante evolución.

1.6.3. Viabilidad Financiera

La viabilidad financiera del estudio sobre ciberdelincuencia y delitos informáticos en el año 2023 es alta debido a la creciente importancia y relevancia de este tema en la actualidad. Con el aumento de la dependencia de la tecnología y la digitalización en todos los ámbitos de la sociedad, la ciberseguridad se ha convertido en una preocupación fundamental para gobiernos, empresas y ciudadanos. Por lo tanto, existe una demanda significativa de investigación en este campo para comprender mejor las amenazas cibernéticas y desarrollar estrategias efectivas para prevenirlas y combatirlas.

Además, el estudio de la ciberdelincuencia y los delitos informáticos en el año 2023 puede generar beneficios tanto económicos como sociales. Por un lado, proporcionará información valiosa para mejorar las medidas de seguridad cibernética y proteger los activos digitales de individuos y organizaciones, lo que a su vez puede ayudar a evitar pérdidas financieras significativas asociadas con ataques cibernéticos. Por otro lado,

contribuirá a la protección de la privacidad y la seguridad de los datos, promoviendo un entorno digital más seguro y confiable para todos. En resumen, invertir en este estudio es una decisión financiera prudente y estratégica dada la importancia y urgencia del tema.

1.6.4. Viabilidad Ambiental

El estudio de la ciberdelincuencia y los delitos informáticos en el año 2023 tiene una viabilidad ambiental significativa, ya que aborda un problema que afecta directamente al entorno digital y, por extensión, al medio ambiente. A medida que la tecnología avanza y se vuelve más omnipresente en nuestras vidas, también lo hacen los riesgos asociados con la delincuencia cibernética, que pueden tener impactos ambientales adversos.

La investigación en este campo puede contribuir a la identificación y mitigación de amenazas digitales que podrían afectar la seguridad de infraestructuras críticas, redes eléctricas, sistemas de suministro de agua y otros recursos vitales. Además, al comprender mejor cómo los delitos informáticos pueden afectar la estabilidad de las operaciones en línea y la confianza en la tecnología, se pueden desarrollar medidas preventivas más efectivas y estrategias de recuperación ante posibles ataques.

Al abordar estos problemas desde una perspectiva ambiental, el estudio de la ciberdelincuencia en el año 2023 puede ayudar a proteger la integridad de los ecosistemas digitales y físicos, promoviendo un entorno más seguro y sostenible para la sociedad y el medio ambiente en general.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Zamora (2011) en su tesis sobre la informática forense en Guatemala, sostiene que la criminalidad informática se expande gracias al anonimato que ofrecen las tecnologías digitales, dificultando la detección de los delincuentes. La legislación guatemalteca aún presenta vacíos significativos que fomentan la impunidad, debido a la falta de actualización normativa y a la escasa capacitación técnica de operadores judiciales. Esta situación evidencia una debilidad institucional en la lucha contra los delitos informáticos. El autor enfatiza la urgencia de reformar el marco legal, fortalecer la formación en informática forense y promover la cooperación internacional. Esta investigación es relevante al demostrar cómo las deficiencias normativas y técnicas pueden limitar severamente la persecución penal en contextos de cibercriminalidad.

Tornel (2022) en su tesis desarrollada en la Universidad Pontificia, advierte sobre el alarmante incremento de la ciberdelincuencia en Europa y España, destacando la ausencia de una definición jurídica uniforme sobre esta figura y sobre las pruebas digitales. Pese a la creación de agencias especializadas en ciberseguridad, la persecución penal enfrenta limitaciones técnicas y normativas, especialmente en lo relativo a la obtención y custodia de evidencia digital. La autora subraya la necesidad

de armonizar la legislación internacional y establecer procedimientos claros que garanticen los derechos fundamentales. Sin una regulación específica, la inseguridad jurídica compromete la eficacia de los procesos judiciales. Este antecedente evidencia la urgencia de una reforma legal integral para enfrentar eficazmente el cibercrimen.

Gómez (2021) en su tesis presentada en la Universidad Rey Juan Carlos, analiza los aspectos procesales vinculados a los delitos informáticos y resalta la importancia de las medidas tecnológicas en la protección de derechos fundamentales como la intimidad y el secreto de las comunicaciones. La reforma procesal de 2015 en España fortaleció garantías en la interceptación de datos, pero persisten desafíos como los descubrimientos casuales y la conservación de datos tras la nulidad de la Directiva 2006/24/CE. El autor destaca el rol clave del juez en la legalidad de las diligencias y la necesidad de colaboración con los operadores tecnológicos. La tesis evidencia el dilema entre la eficacia investigativa y la protección de la privacidad en el entorno digital.

Ochoa (2021) en su investigación sobre el cibercrimen en Ecuador entre 2014 y 2019, advierte que la ausencia de políticas públicas sólidas ha dejado a la ciudadanía vulnerable frente a delitos informáticos. Aunque se tipificaron los delitos informáticos en el Código Penal en 2014, persisten deficiencias en la investigación y persecución penal. El autor resalta que la protección de datos personales no puede depender exclusivamente del sector privado, debido a posibles abusos, como ocurrió en el caso Novaestrat. Propone una articulación efectiva entre el sector público y privado, mediante leyes específicas e instituciones autónomas de control.

Además, urge una cooperación internacional real para enfrentar la transnacionalidad del cibercrimen y garantizar la seguridad de la información digital.

Rodríguez (2018) en su tesis sobre la tipificación de delitos informáticos en redes sociales, propone una metodología de clasificación técnica que permite identificar vacíos legales en el marco jurídico ecuatoriano. El autor analiza cómo el uso masivo de plataformas como Facebook o YouTube ha incrementado la vulnerabilidad de los usuarios frente a nuevas formas de ciberdelito. Mediante una estructura metodológica organizada, logra distinguir entre conductas sancionadas y aquellas aún no contempladas por la ley. Asimismo, plantea que la sociedad civil puede participar activamente en la formulación de propuestas legislativas en ciberseguridad. Su estudio concluye que la falta de tipificación específica impide una respuesta jurídica eficaz y que se requieren leyes claras para proteger derechos en entornos digitales.

2.1.2. Antecedentes nacionales

Carbajal (2022), en su tesis sobre fiscalías especializadas en delitos informáticos, evidencia que entre 2013 y 2020 el fraude informático fue la modalidad más frecuente en Perú, destacando prácticas como clonación de tarjetas, compras fraudulentas y transferencias no autorizadas. Sin embargo, muchas de estas conductas no están expresamente tipificadas en la Ley Nº 30096, lo que limita la capacidad sancionadora del sistema penal. La falta de adecuación normativa y de personal capacitado obstaculiza la labor de entidades como la División de Delitos de Alta

Tecnología. El autor plantea la necesidad urgente de reformas legislativas y de inversión en infraestructura y formación especializada para enfrentar de forma eficaz el crecimiento acelerado de la ciberdelincuencia en el país.

Morales (2016) en su tesis sobre delitos informáticos en redes sociales, advierte que el vertiginoso avance de la computación ha generado, junto a sus beneficios, nuevas formas de criminalidad digital difíciles de prever por el marco legal vigente. La falta de adecuación legislativa y las contradicciones con normas como el Código Penal complican la sanción de estos delitos. El autor resalta que la delincuencia informática se vale de la conectividad global y el anonimato para vulnerar datos personales, y que su combate requiere legislación moderna, recursos técnicos suficientes y apoyo de la criminalística. La tesis concluye que sin una respuesta jurídica integral, la evolución tecnológica seguirá superando la capacidad del Estado para proteger a los ciudadanos en entornos digitales.

Chiriboga (2021) en su tesis desarrollada en el distrito de Comas, evidencia la preocupante vinculación entre la ciberdelincuencia y los delitos contra la libertad sexual, especialmente en perjuicio de menores de edad. Señala que las redes sociales permiten a los agresores establecer vínculos de confianza con sus víctimas para luego ejercer chantaje, hostigamiento o acoso sexual. El impacto psicológico del ciberacoso es devastador, generando en los menores ansiedad, aislamiento social e incluso pensamientos suicidas. El autor exige una respuesta legal y social inmediata, que incluya políticas de ciberseguridad, regulación estricta de plataformas digitales y apoyo a las víctimas. La tesis concluye que solo un

enfoque integral permitirá frenar este tipo de violencia digital en expansión.

Ventura (2021), en su tesis sobre la tipificación del phishing, smishing y vishing en el sistema penal peruano, advierte que la legislación vigente no contempla expresamente estas modalidades de ciberdelito, a pesar de su peligrosidad y frecuencia. Esta omisión legal ha permitido su proliferación, agravada por la falta de prevención estatal y bancaria. El autor propone clasificarlos como delitos de peligro abstracto o delitos de resultado, según su impacto, y resalta la necesidad de proteger tanto la seguridad informática como los derechos de los usuarios. Concluye que las deficiencias legislativas e institucionales dificultan la persecución efectiva, y exige una reforma normativa urgente, junto con la mejora de infraestructura y capacitación especializada en ciberseguridad y persecución penal.

Huamán (2020) en su tesis sobre los delitos informáticos y el Convenio de Budapest, sostiene que este tratado internacional ha impulsado avances normativos en el Perú, como la Ley 30171, permitiendo una legislación más alineada con estándares internacionales. No obstante, la cooperación internacional aún es mínima, y los delitos informáticos siguen creciendo debido al uso avanzado de tecnología por parte de los delincuentes. El autor identifica como principal obstáculo la escasez de recursos económicos y tecnológicos para una persecución penal efectiva. Aunque el convenio ha favorecido la uniformidad legislativa en la región, se requiere fortalecer la infraestructura digital del Estado y articular acciones conjuntas con otros países firmantes para enfrentar la ciberdelincuencia de manera efectiva.

2.1.3. Antecedentes locales

Marín y Santa Maria (2021) en su tesis sobre ciberdelito y control interno en municipalidades de Ucayali, evidencian una fuerte correlación entre los riesgos tecnológicos y la necesidad de implementar auditorías antifraude. El 92% de los encuestados afirmó que el uso de tecnología sin adecuados mecanismos de control incrementa la exposición a fraudes, robos de identidad y desvío de fondos. Asimismo, se destaca la urgencia de fortalecer la seguridad de los sistemas informáticos y proteger la integridad de los funcionarios públicos frente a ataques cibernéticos. Los resultados respaldan la implementación de políticas preventivas y mecanismos de control interno como estrategia clave para garantizar la transparencia y la correcta gestión de los recursos públicos en el ámbito municipal.

Díaz y Huamán (2022), en su tesis desarrollada en Coronel Portillo, revelan una estrecha relación entre el lavado de dinero y diversas formas de criminalidad organizada, especialmente mediante el uso de criptomonedas. La correlación entre lavado de activos y crimen organizado alcanzó un coeficiente de 0.79, evidenciando su gravedad. Asimismo, se identificaron vínculos significativos con el tráfico de drogas (0.55), trata de personas (0.42), minería ilegal (0.55) y cripto criminalidad (0.51). Estos hallazgos sugieren que el dinero digital facilita el financiamiento ilícito de actividades delictivas complejas. La investigación concluye que se requieren estrategias integrales de fiscalización financiera y reformas legislativas orientadas a controlar la circulación de activos digitales en contextos de alta vulnerabilidad criminal.

Cataño y Panduro (2023) en su tesis sobre la incidencia del delito informático en los bancos de Coronel Portillo, evidencian una correlación positiva fuerte (Rho = 0.756) entre esta actividad delictiva y las operaciones financieras. Asimismo, identifican vínculos significativos con el phishing (0.553), la gestión de riesgos (0.685) y la vulnerabilidad de los créditos otorgados (0.850). Estos resultados demuestran que el delito informático representa una amenaza directa para la estabilidad del sistema bancario en la región. El estudio destaca la necesidad urgente de fortalecer los protocolos de seguridad digital, así como de diseñar estrategias preventivas que protejan los datos financieros y mitiguen el impacto del fraude en las instituciones financieras locales.

2.2. Bases teóricas

2.2.1. Delitos informáticos

El avance vertiginoso de las Tecnologías de Información y Comunicación (TIC) ha transformado drásticamente la sociedad en los últimos quince años. Estas variaciones son constantes y rápidas, moldeando los enfoques tradicionales de la vida cotidiana. Los seres humanos se adaptan a estos cambios, adoptando nuevas técnicas y utilizando la tecnología diariamente en beneficio de la sociedad. Sin embargo, es fundamental que este uso no viole los derechos de terceros.

Desafortunadamente, el Internet y los medios electrónicos también han sido aprovechados para cometer delitos o para vulnerar la seguridad, lo que puede generar perjuicios significativos en la sociedad. Estas

acciones perjudiciales se conocen como delitos informáticos, cibercrimen o ciberdelitos, y deben ser severamente sancionadas.

Es crucial reconocer que, si bien las TIC han brindado numerosos beneficios, también han creado nuevos desafíos en términos de seguridad y ética. Es responsabilidad de los individuos y de las autoridades garantizar que el uso de la tecnología sea ético y no cause daño a otros.

En este sentido, la prevención y la aplicación efectiva de la ley son fundamentales para combatir el cibercrimen y proteger a la sociedad en su conjunto. Esto implica una cooperación internacional y una legislación actualizada que se adapte a los constantes avances tecnológicos.

El avance de las TIC (Tecnología Informática y Comunicación) ha transformado la sociedad de manera significativa, ofreciendo oportunidades y desafíos. Es esencial que el uso de la tecnología se realice de manera responsable y ética, evitando así el daño a terceros y garantizando un entorno digital seguro para todos (Rayón y Gómez, 2014).

2.2.2. La clasificación de los delitos informáticos

Los delitos informáticos han surgido como una preocupación creciente en la era digital, planteando desafíos complejos tanto para la ley como para la sociedad en su conjunto. La clasificación de estos delitos como herramientas o como objetivos reales refleja la diversidad y la sofisticación de las actividades delictivas en el ámbito digital.

Es importante comprender que los delitos informáticos pueden ser utilizados como instrumentos para llevar a cabo actos delictivos convencionales. Esto implica el uso de tecnología y técnicas informáticas

para facilitar la comisión de delitos como la estafa, el fraude financiero o incluso el asesinato. En este sentido, la informática se convierte en una herramienta poderosa para aquellos que buscan perpetrar actos ilícitos, aprovechando la complejidad y la interconexión de los sistemas informáticos.

Por otro lado, los delitos informáticos también pueden ser cometidos directamente contra sistemas informáticos o programas. Esto incluye actividades como la alteración de documentos digitales, el robo de información confidencial, el acceso no autorizado a sistemas informáticos y la manipulación de datos. Estas acciones no solo pueden causar daños económicos significativos, sino que también representan una amenaza para la seguridad y la integridad de los sistemas informáticos en general.

La clasificación y la codificación de los delitos informáticos son fundamentales para poder abordar adecuadamente este tipo de actividades ilegales. Al definir claramente qué acciones constituyen un delito informático, las autoridades pueden desarrollar estrategias efectivas de prevención y aplicación de la ley. Además, la legislación específica en materia de delitos informáticos ayuda a crear conciencia sobre la gravedad de estas acciones y disuade a posibles infractores.

El bien jurídico que se protege en el contexto de los delitos informáticos es la integridad y la seguridad de los sistemas informáticos y de la información que contienen. Esto incluye la protección de datos personales, la seguridad de las transacciones financieras y la confidencialidad de la información empresarial. Al garantizar la seguridad

de estos sistemas, se promueve la confianza en la tecnología y se protege a los usuarios contra posibles abusos.

Los delitos informáticos representan una amenaza significativa en la sociedad actual, tanto como herramientas para cometer delitos convencionales como en su forma directa de ataques contra sistemas informáticos. La clasificación y la codificación de estos delitos son fundamentales para combatirlos de manera efectiva y proteger la integridad de los sistemas informáticos y la información que contienen. Es crucial que las autoridades y la sociedad en su conjunto estén alertas ante estas amenazas y tomen medidas proactivas para prevenirlas y sancionarlas adecuadamente (Rodríguez, 2020).

2.2.3. Tipicidad de los delitos informáticos

La tipicidad en el ámbito jurídico se refiere a la cualidad de una conducta que se ajusta al tipo penal establecido por la ley. En otras palabras, una conducta es típica cuando encaja dentro de la descripción que la ley penal proporciona. Esta definición implica distinguir entre el tipo objetivo, que se refiere a la actividad en sí misma, y la tipología subjetiva, que se relaciona con el elemento del dolo en la conducta del individuo.

Cuando se habla de tipicidad en relación con los delitos informáticos, se está haciendo referencia a la necesidad de establecer tipos penales específicos para los delitos cometidos con el uso de tecnologías informáticas. Estos delitos informáticos han surgido como una nueva forma de criminalidad en la era digital, aprovechando las vulnerabilidades y las oportunidades que ofrece la tecnología.

El estudio de la tipicidad en los delitos informáticos implica analizar y fundamentar la naturaleza ilícita de las conductas que se llevan a cabo en el contexto digital. Esto requiere un examen cuidadoso de cómo las actividades delictivas se adaptan a las disposiciones legales existentes y cómo pueden ser tipificadas de manera adecuada para su procesamiento legal.

Los delitos informáticos abarcan una amplia gama de actividades, que van desde el acceso no autorizado a sistemas informáticos hasta el robo de información confidencial y la manipulación de datos. Estas acciones pueden tener graves consecuencias tanto para los individuos como para las organizaciones, lo que subraya la importancia de establecer una tipología clara y precisa para este tipo de delitos.

Además, la tipicidad en los delitos informáticos también implica considerar la evolución constante de la tecnología y su impacto en las formas en que se cometen los delitos. Los cambios en el panorama tecnológico pueden requerir ajustes en la legislación y en las estrategias de aplicación de la ley para abordar de manera efectiva las nuevas formas de delincuencia digital.

La tipicidad en los delitos informáticos es un aspecto crucial del derecho penal moderno, que busca establecer tipos penales específicos para las actividades delictivas en el ámbito digital. Este análisis requiere una comprensión profunda de la tecnología y su impacto en la sociedad, así como una adaptación constante a los cambios en el panorama tecnológico para garantizar la eficacia de las leyes y políticas de aplicación de la ley (López, 2021).

2.2.4. Tipicidad objetiva de los delitos informáticos

La tipicidad objetiva en el ámbito del derecho penal busca determinar de manera precisa la lesión causada a un bien jurídico, evaluando si dicha lesión es el resultado de una acción deliberada o simplemente una consecuencia fortuita. Al examinar la legislación vigente, encontramos que la tipicidad objetiva de los delitos informáticos se define por una serie de características específicas, como el objeto del delito, los sujetos involucrados, la acción típica, la causalidad, la imputabilidad objetiva y los elementos descriptivos legales correspondientes a este tipo de delitos.

En el contexto de los delitos informáticos, existen diversas categorías, que van desde los delitos contra sistemas y datos informáticos hasta las infracciones contra la intimidad sexual, la propiedad o el patrimonio, y las transgresiones contra la fe pública. La acción típica, como elemento esencial del aspecto objetivo del tipo legal, se define por la operación descrita por el verbo principal en la normativa aplicable. Por ejemplo, en los delitos informáticos contra la autonomía sexual, la acción típica puede consistir en el establecimiento de relaciones a través de Internet con personas menores de edad, siendo punible incluso la mínima intención de conexión.

En cuanto al nexo de causalidad, este se establece como una cualidad jurídica y social que busca vincular el acto delictivo con su autor. Es crucial que exista una correspondencia entre la acción y sus consecuencias, y en el caso de los delitos informáticos, esta conexión se

determina mediante pruebas virtuales que ubican al autor en el acto delictivo.

La imputación objetiva, por su parte, implica la atribución de responsabilidad al autor del delito en el marco del tipo legal establecido. En los delitos informáticos, las penas pueden variar entre 1 y 8 años de prisión, dependiendo de la gravedad de la acción perpetrada.

Los factores legales y descriptivos son elementos independientes entre sí, siendo los factores descriptivos definiciones tomadas del lenguaje común que deben ser verificadas por el juez, mientras que los factores legales requieren una evaluación de valor. En el caso de los delitos informáticos, es crucial establecer correctamente los verbos principales o directos para comprender los elementos descriptivos de estas acciones delictivas específicas.

La tipicidad objetiva en los delitos informáticos se basa en una serie de características específicas, que incluyen el objeto del delito, la acción típica, el nexo causal, la imputabilidad objetiva y los elementos descriptivos legales. Es fundamental entender estos aspectos para aplicar adecuadamente la ley en el contexto de los delitos informáticos y garantizar una justicia efectiva en el ámbito digital (Espinoza, 2022).

2.2.5. Sujetos de los delitos informáticos

El estudio de los elementos que intervienen en los delitos informáticos es fundamental para comprender la complejidad de este fenómeno en la sociedad moderna. En particular, la consideración de los

sujetos activos y pasivos en estos actos delictivos revela la diversidad de actores y motivaciones que están en juego en el ámbito digital.

El sujeto activo en los delitos informáticos representa a aquel individuo que comete el ciberdelito, y su perfil difiere notablemente del delincuente tradicional. Según Hidalgo y Solano (2021), estos individuos poseen habilidades específicas en el manejo de sistemas informáticos, y suelen ocupar posiciones laborales que les otorgan acceso privilegiado a información sensible. No se trata de delincuentes comunes, cuya identificación podría ser relativamente sencilla, sino de individuos que operan tras una serie de códigos y que tienen una comprensión binaria del entorno digital. Su destreza técnica plantea desafíos éticos y educativos, y su capacidad para sortear sistemas de seguridad genera debates sobre la regulación y el acceso a este tipo de conocimientos.

Dentro de esta categoría de sujetos activos, se distingue entre los denominados hackers y crackers. Los hackers, en muchos casos, son profesionales contratados por empresas para evaluar la vulnerabilidad de sus sistemas y proponer mejoras. Por otro lado, los crackers son individuos que utilizan sus habilidades informáticas de manera maliciosa, accediendo a sistemas remotos con la intención de causar daño o alterar datos.

Por otro lado, el sujeto pasivo en los delitos informáticos es la víctima de la acción delictiva. Esta puede ser una persona, una empresa o una institución que sufre daños directos o indirectos como resultado de la actividad del sujeto activo. El incremento de casos de delitos informáticos ha puesto de relieve la importancia de proteger a estos sujetos pasivos y

de implementar medidas de seguridad adecuadas para prevenir este tipo de ataques.

Es crucial entender que la relación entre el sujeto activo y pasivo en los delitos informáticos es compleja y dinámica. La evolución constante de la tecnología y las estrategias de seguridad plantea desafíos continuos para las autoridades y las empresas en la lucha contra este tipo de delitos. Solo mediante un enfoque integral que comprenda tanto los aspectos técnicos como legales y éticos, será posible abordar eficazmente esta problemática y proteger la integridad de los sistemas informáticos y la información que contienen.

2.2.6. Delincuente informático

Los delincuentes informáticos, según Mengoa (2021), suelen ser personas de confianza con acceso al sistema informático. Esto destaca la importancia de la seguridad en la gestión de empleados y la protección de datos sensibles. Las estadísticas revelan que la mayoría de los delitos son perpetrados por usuarios del sistema, lo que subraya la necesidad de una vigilancia proactiva y medidas de seguridad robustas. Estos individuos tienen un profundo conocimiento de las vulnerabilidades del sistema y saben cómo explotarlas para acceder o destruir información. Por lo tanto, la prevención y la educación son clave para mitigar los riesgos asociados con el ciberdelito y proteger la integridad de los datos.

2.2.7. Tipicidad subjetiva de los delitos informáticos

La tipicidad subjetiva, según Custodio (2021), se relaciona con la culpabilidad y el dolo, siendo fundamental para determinar si un acto delictivo se ajusta al tipo penal. En delitos informáticos, es esencial establecer la intención detrás de la conducta para determinar su tipicidad. La Ley de Delitos Informáticos, en su artículo 5, aborda este aspecto, describiendo un propósito específico del agente más allá del dolo (Villavicencio, 2014) destaca la intención de obtener ciertos resultados, como material pornográfico, lo que implica una aproximación deliberada al delito, especialmente si el sujeto pasivo es un menor de edad. Este enfoque subjetivo es crucial para comprender y combatir eficazmente los delitos informáticos.

2.2.8. Delitos informáticos

El avance de las Tecnologías de la Información y la Comunicación (TIC) ha marcado un cambio significativo en la sociedad, transformando nuestras vidas en un período de tan solo quince años. Estas transformaciones son constantes y rápidas, remodelando continuamente nuestra forma de vida. Los seres humanos se adaptan a estas variaciones, adoptando nuevas tecnologías y utilizándolas diariamente en beneficio de la sociedad, siempre y cuando no infrinjan los derechos de otros individuos.

Sin embargo, lamentablemente, el uso del Internet y los medios electrónicos también ha dado lugar a actividades delictivas y vulneraciones que pueden afectar y perjudicar a la sociedad. Estos comportamientos

dañinos se conocen como delitos informáticos, cibercrimen o ciberdelitos. Estos delitos no solo son perpetrados por individuos comunes, sino que también han sido adoptados por organizaciones criminales altamente capacitadas en tecnologías de la información.

La ciberseguridad y el ciberdelito están intrínsecamente relacionados en un mundo interconectado. La resolución de la Asamblea General de las Naciones Unidas de 2010 sobre Ciberseguridad aborda esta relación y reconoce la importancia de combatir el ciberdelito a nivel global, dado que el ciberespacio no tiene fronteras definidas y el uso de tecnologías informáticas está globalizado.

El combate contra el delito informático presenta desafíos considerables, como la identificación de los autores y la falta de cooperación internacional efectiva. Además, muchos expertos señalan que el cibercrimen puede ser más lucrativo que el tráfico de drogas, moviendo millones de dólares anuales.

La jurisdicción sobre los delitos informáticos en el ciberespacio es un tema complejo, ya que los autores pueden estar ubicados en diferentes partes del mundo y los servicios utilizados pueden ser proporcionados por una variedad de proveedores internacionales. Por lo tanto, la determinación de un tribunal competente para juzgar estos delitos se convierte en un desafío crucial en la lucha contra el ciberdelito.

Los delitos informáticos representan una amenaza seria y global en la sociedad moderna. La cooperación internacional, la actualización de la legislación y la mejora de las capacidades de aplicación de la ley son fundamentales para abordar eficazmente este problema y proteger a la

sociedad contra los riesgos del ciberespacio (Canedo, 2010).

2.2.9. Uso de la información en el internet

La introducción de nuevas técnicas de comunicación e información ha transformado profundamente los sistemas educativos en todo el mundo, impactando tanto en la infraestructura escolar como en los métodos de enseñanza. La evolución de la Web 2.0 ha permitido un acceso sin precedentes a una variedad de recursos educativos, desde bibliotecas digitales hasta plataformas comerciales en línea. Sin embargo, en el ámbito escolar, esta revolución tecnológica ha enfrentado obstáculos relacionados con la adaptación de los contextos prácticos y pedagógicos a las nuevas formas de información.

El surgimiento de Internet en 1969 marcó el inicio de una era de comunicación y tecnología sin precedentes, brindando una plataforma para la integración de la comunicación y la técnica. A lo largo del tiempo, Internet ha crecido exponencialmente en todo el mundo, convirtiéndose en una herramienta indispensable que ha facilitado el avance tecnológico en diversas áreas. Sin embargo, según Oxman (2013) la utilización del internet en el contexto educativo aún se encuentra en proceso de adaptación, enfrentando desafíos en la integración efectiva de las tecnologías de la información y la comunicación (TIC) en el aula.

La implementación de experiencias educativas con TIC, según Rincón (2015), ha demostrado ser beneficiosa para el aprendizaje y el desarrollo de habilidades relevantes para el siglo XXI. La accesibilidad a la información y el uso repetido en la producción y el aprendizaje han

generado la necesidad de promover la alfabetización digital, como menciona la UNESCO (2008), con el objetivo de capacitar a los estudiantes y a la comunidad en general en el uso de nuevas tecnologías.

El desarrollo de habilidades informacionales y el fomento del pensamiento autónomo y creativo son aspectos clave para preparar a los alumnos para enfrentar los desafíos del mundo moderno, En el contexto escolar, el uso apropiado de Internet por parte de profesores y alumnos es fundamental para maximizar los beneficios educativos y reducir los riesgos asociados con el acceso no adecuado a la información. La formación docente en el uso de TIC y la promoción de habilidades informáticas entre los estudiantes son aspectos esenciales para garantizar un uso responsable y efectivo de la tecnología en el aula.

La integración de las TIC en el ámbito educativo presenta oportunidades y desafíos significativos. La capacitación adecuada de docentes y alumnos, así como la promoción de una cultura de uso responsable de la tecnología, son pasos clave para aprovechar al máximo el potencial educativo de Internet y otras herramientas digitales (Leyva, 2021).

2.2.10. El uso del Internet y las competencias informacionales

El perfeccionamiento de competencias informacionales es esencial en la sociedad actual, donde el acceso y la gestión de la información son fundamentales para la competitividad y el éxito, (Mayer y Oliver, 2020) destacan la importancia de cuatro tipos de competencias informacionales:

potencializante, virtualizante, actualizante y realizante. Estas competencias guían el proceso de adquisición, manejo y comunicación de la información, facilitando el aprendizaje y la toma de decisiones informadas.

En este contexto, la ciberdelincuencia emerge como una preocupación creciente en la sociedad contemporánea. Con el avance tecnológico, los delincuentes han encontrado nuevas formas de cometer crímenes, aprovechando las vulnerabilidades de los sistemas informáticos y de comunicación. El Convenio sobre la Ciberdelincuencia, celebrado en Huamán (2020), define este fenómeno como aquel dirigido a comprometer la confidencialidad, integridad y disponibilidad de los sistemas informáticos y datos.

La ciberdelincuencia abarca una amplia gama de actividades delictivas, desde el acceso no autorizado a sistemas informáticos hasta el robo de datos y la manipulación de tecnologías de la información y comunicación. Su naturaleza digital permite a los delincuentes actuar de manera global, sin restricciones geográficas, lo que representa un desafío significativo para la aplicación de la ley y la seguridad cibernética.

Los ciberdelincuentes pueden operar de manera individual, como parte de organizaciones criminales o incluso con el respaldo financiero de estados o entidades poderosas. Esta diversidad de actores y motivaciones complica aún más la lucha contra este tipo de crimen, ya que requiere una respuesta coordinada a nivel internacional y una constante adaptación a las nuevas amenazas y técnicas utilizadas por los delincuentes.

Para combatir eficazmente la ciberdelincuencia, es fundamental fortalecer la seguridad cibernética, promover la conciencia y la educación digital, y mejorar la colaboración entre gobiernos, empresas y sociedad civil. Esto incluye el desarrollo de legislación adecuada, la capacitación de profesionales en ciberseguridad y la promoción de buenas prácticas en el uso de la tecnología.

La ciberdelincuencia representa un desafío multifacético en la era digital, que requiere respuestas integrales y coordinadas a nivel nacional e internacional. El perfeccionamiento de competencias informacionales y la promoción de una cultura de seguridad cibernética son clave para proteger la integridad de los sistemas informáticos y garantizar un uso seguro y ético de la tecnología en la sociedad actual.

2.2.11. Delitos de sustracción de datos personales, suplantación de identidad y extorsión

En el contexto actual, los delitos informáticos, como la sustracción de datos personales, la suplantación de identidad y la extorsión, han proliferado debido al avance de la tecnología y la creciente dependencia de la sociedad en el ámbito digital. Estos delitos representan una amenaza seria para la seguridad y privacidad de las personas, así como para la integridad de las instituciones y empresas.

La sustracción de datos personales es una práctica común entre los ciberdelincuentes, quienes acceden ilegalmente a información confidencial con el objetivo de utilizarla para cometer fraudes o extorsionar a las

víctimas. Este tipo de delito puede tener consecuencias devastadoras para los afectados, ya que puede resultar en el robo de identidad, la pérdida de información sensible o el acceso no autorizado a cuentas bancarias y financieras.

La suplantación de identidad, por otro lado, implica el uso fraudulento de la identidad de otra persona para llevar a cabo actividades ilícitas, como la realización de transacciones financieras fraudulentas, el acceso ilegal a sistemas informáticos o la difusión de información falsa. Este tipo de delito socava la confianza en las instituciones y en el sistema de justicia, y puede tener consecuencias graves para las víctimas.

La extorsión es otro delito informático que ha aumentado en frecuencia en los últimos años. Los ciberdelincuentes utilizan diversas técnicas, como el ransomware o el phishing, para extorsionar dinero u obtener beneficios económicos de sus víctimas. Este tipo de delito puede tener un impacto significativo en la economía y la estabilidad financiera de las empresas y organizaciones afectadas.

Ante esta situación, es fundamental que la legislación vigente sobre delitos informáticos se actualice y se fortalezca para abordar de manera efectiva estas nuevas modalidades delictivas. Es necesario incorporar disposiciones específicas que tipifiquen y sancionen adecuadamente la sustracción de datos personales, la suplantación de identidad y la extorsión en el ámbito digital.

La actualización de la legislación sobre delitos informáticos debe contemplar medidas que permitan una investigación y persecución eficaz de estos delitos, así como la protección de las víctimas y la prevención de

futuros ataques. Esto incluye la implementación de mecanismos de denuncia y seguimiento, el fortalecimiento de la cooperación internacional en materia de ciberseguridad y la promoción de la conciencia pública sobre los riesgos y peligros asociados con el uso de la tecnología.

La sustracción de datos personales, la suplantación de identidad y la extorsión son delitos informáticos que representan una amenaza creciente en el mundo digital actual. Es crucial que la legislación vigente se actualice y se fortalezca para enfrentar estos desafíos y garantizar la seguridad y protección de los ciudadanos en el entorno digital (Bank, 2020).

2.2.12. Ciberamenazas y Ciberextorsión

Las amenazas y la extorsión han sido siempre tácticas comunes empleadas por los delincuentes para obtener beneficios a expensas de sus víctimas. Sin embargo, con el avance de la tecnología, estas prácticas delictivas han encontrado un nuevo escenario en el ciberespacio, donde los criminales pueden operar con mayor impunidad y proteger su anonimato. Este cambio de paradigma representa un desafío significativo para las pequeñas y medianas empresas, que cuentan con recursos limitados para invertir en ciberseguridad son más susceptibles a ataques debido a sus vulnerabilidades.

De acuerdo con Temperini (2013), los delitos cibernéticos, especialmente las amenazas y coacciones, han aumentado notablemente en los últimos años, convirtiéndose en una preocupación importante para empresas y organizaciones de todos los sectores. Estos delitos se

encuentran entre los más frecuentes después de los fraudes informáticos, lo que subraya la importancia de abordar este problema de manera proactiva.

El phishing y el ransomware son dos técnicas ampliamente utilizadas por los ciberdelincuentes para llevar a cabo amenazas y extorsiones tanto a nivel empresarial como individual. El phishing implica el envío de correos electrónicos fraudulentos con el objetivo de obtener información confidencial, mientras que el ransomware bloquea el acceso a los sistemas informáticos y exige un rescate para restablecer el acceso.

Para una empresa u organización pública, la interrupción de sus sistemas informáticos puede tener consecuencias devastadoras, provocando pérdidas económicas y daños en su reputación. Los ciberdelincuentes son conscientes de esto y aprovechan la urgencia de restablecer los sistemas para extorsionar a sus víctimas de manera más efectiva.

Además, la sustracción de información sensible por parte de hackers también se utiliza como una herramienta de amenaza y extorsión. Los delincuentes amenazan con divulgar esta información en línea si no se cumplen sus demandas, lo que añade una capa adicional de presión sobre las víctimas.

Como se ha destacado a lo largo de este ensayo, la información es un recurso valioso en la era digital, y aquellos que la poseen tienen un poder considerable sobre los demás. Por lo tanto, es crucial que las empresas y organizaciones implementen medidas efectivas de ciberseguridad para proteger sus sistemas y datos contra amenazas y

extorsiones cibernéticas.

Las amenazas y la extorsión son formas de delito que han evolucionado con el avance de la tecnología, encontrando un nuevo terreno fértil en el ciberespacio. Las empresas y organizaciones deben tomar medidas proactivas para protegerse contra estos ataques y garantizar la seguridad de sus sistemas y datos en un entorno digital cada vez más complejo y peligroso (Cárdenas, 2008)

2.2.13. Grooming, sexting, ciberbulling y ciberacoso

El grooming, una táctica empleada por los ciberdelincuentes sexuales, representa una seria amenaza en la era digital. Con la proliferación de redes sociales y aplicaciones de mensajería, tanto menores como adultos están expuestos a este tipo de peligros. Los menores, en particular, son especialmente vulnerables debido a su acceso descontrolado y no supervisado en línea (Hidalgo y Solano, 2021).

El proceso de grooming implica que los delincuentes se oculten tras una identidad falsa para entablar conversaciones con menores en plataformas como Instagram, Facebook o TikTok. Aprovechando la inocencia y la falta de experiencia de los jóvenes, los depredadores buscan obtener información personal y, eventualmente, coaccionarlos para acceder a su sexualidad.

Por otro lado, el sexting, un delito relacionado, implica el intercambio de contenido íntimo entre individuos de confianza, que luego es difundido sin consentimiento. Cuando estos delitos se combinan, el riesgo para la víctima aumenta exponencialmente. Además, se suma el ciberbullying y el

ciberacoso, donde la víctima es intimidada, humillada o avergonzada a través de plataformas digitales.

Los ciberdelincuentes no dudan en utilizar imágenes íntimas obtenidas de forma fraudulenta para chantajear a sus víctimas y obligarlas a realizar acciones no deseadas. Este círculo vicioso de abuso y manipulación es profundamente perturbador y puede dejar secuelas psicológicas de por vida en las víctimas.

Es fundamental que la sociedad tome conciencia de estos peligros y adopte medidas para proteger a los menores en línea. La educación sobre seguridad en Internet debe ser una prioridad tanto en los hogares como en las instituciones educativas. Los padres y tutores deben supervisar de cerca la actividad en línea de los jóvenes y establecer reglas claras sobre el uso de Internet.

Las plataformas en línea también deben asumir su responsabilidad y tomar medidas para prevenir y abordar el grooming y otros comportamientos delictivos en línea. La implementación de políticas de privacidad más estrictas y la colaboración con las autoridades para identificar y detener a los delincuentes son pasos cruciales en esta lucha.

El grooming y otros delitos sexuales en línea representan una grave amenaza para la seguridad de los menores en la era digital. Es necesario un esfuerzo colectivo para proteger a los jóvenes y garantizar un entorno en línea seguro y saludable para todos.

2.2.14. Suplantación de identidad a empresas y sustracción de datos

Durante la pandemia, las plataformas de renombre como Google, Facebook e Instagram se han convertido en blancos prioritarios para los ciberdelincuentes que buscan suplantar la identidad de marcas reconocidas para difundir anuncios falsos. Este fenómeno no solo tiene como objetivo instalar malware, sino también estafar a los usuarios desprevenidos.

Uno de los métodos más utilizados por los ciberdelincuentes es la creación de dominios maliciosos y la realización de ataques de phishing y malware. Durante la crisis sanitaria, el interés público se centró en buscar información relacionada con el COVID – 19, lo que los delincuentes aprovecharon para posicionar páginas web fraudulentas utilizando términos como "Covid19", "coronavirus" y similares. Estas páginas se utilizan para distribuir spam o realizar ataques de phishing, aprovechando la confusión de los usuarios y su falta de discernimiento entre sitios web legítimos e ilegales.

La falta de conocimiento por parte de los usuarios sobre cómo identificar sitios web fraudulentos los hace vulnerables a caer en trampas, proporcionando involuntariamente sus datos personales a los ciberdelincuentes. Se han reportado casos de malware, spyware y troyanos en páginas web que ofrecen información sobre el COVID-19, así como en mapas interactivos relacionados con la pandemia.

Además, durante la crisis sanitaria, se han incrementado los ataques de ransomware dirigidos a centros sanitarios, instituciones públicas y compañías de seguros. Estos ataques han provocado bloqueos

en los sistemas informáticos, afectando la capacidad de respuesta ante la emergencia sanitaria y generando graves consecuencias para la población afectada por el virus.

Es importante destacar que estos ataques cibernéticos han afectado a instituciones que desempeñan un papel crucial durante la pandemia y que no pueden permitirse interrupciones en su funcionamiento. Los centros sanitarios, en particular, han enfrentado dificultades adicionales debido a los ataques de ransomware, lo que ha puesto en peligro la atención médica y la seguridad de los pacientes (Rodríguez, 2020).

La pandemia ha exacerbado la actividad de los ciberdelincuentes, que aprovechan la crisis para perpetrar ataques dirigidos a instituciones y usuarios vulnerables. Es fundamental que los usuarios estén alerta y tomen medidas de seguridad adicionales al navegar por Internet, especialmente al buscar información relacionada con la salud pública. Asimismo, es necesario que las autoridades y las empresas refuercen sus sistemas de seguridad cibernética para protegerse contra estos ataques cada vez más sofisticados y peligrosos (Gómez, 2019).

2.3. Definición de términos básicos

- **Concurso ideal de delitos:** El concurso ideal de delitos es una figura del derecho penal que se refiere a la concurrencia de dos o más tipos delictivos en un mismo acto o conducta, donde cada uno de ellos se encuentra plenamente consumado. En otras palabras, se trata de la comisión de varios delitos de manera simultánea y autónoma, sin que ninguno de ellos dependa del otro para su

existencia o consumación. En este caso, el sujeto activo es responsable de cada uno de los delitos por separado, y la pena que enfrenta puede ser determinada de acuerdo con la suma de las penas correspondientes a cada delito, con ciertos límites establecidos por la ley (Álvarez, 2007).

- **Concurso real de delitos:** El concurso real de delitos se refiere a la situación en la que una persona comete dos o más delitos de forma independiente, es decir, sin que uno sea consecuencia del otro. Cada delito se considera como una unidad jurídica separada, y el autor es sancionado por cada uno de ellos de manera individual, sin que se fusionen las penas. En el concurso real, las penas por cada delito se suman, lo que puede resultar en una pena total más severa que si los delitos se hubieran cometido de manera aislada. (Álvarez, 2007).

- **Datos informáticos:** “Toda imagen de vicisitudes, indagación mencionados de cualquier modo que se preste a procedimiento informático, comprendidos los programas esbozados para que un régimen informático realice una función”. (Barrera, 2017)

- **Delito:** “Se refiere a una conducta intencional o culpable, contraria a la ley y que se ajusta a lo establecido como delito, y que por ende puede ser castigada legalmente”. (Lamperti, 2017)

- **Falsedad:** “La falta de medios o métodos para verificar la veracidad o validez de lo que se está evaluando o juzgando”. (Quiroz, 2018)

- **Falsificación:** “La falsificación es el acto de crear o alterar documentos, productos o servicios con la intención de hacerlos parecer genuinos o de modificar la verdad”. (Quiroz, 2018)

- **Informática: “**El término se refiere a un conjunto de conocimientos científicos y tecnológicos que permiten el procesamiento automático de información a través de computadoras”. (Proaño y Gavilanes, 2019)

- **Internet:** Una red internacional descentralizada que facilita la comunicación directa entre computadoras y otros dispositivos mediante un protocolo específico, el TCP/IP. Su propósito es permitir a los usuarios acceder al "ciberespacio" y obtener una amplia cantidad de información de todo el mundo. (Mata, 2007)

- **Libertad Informática:** La esfera de libertad personal en el contexto de la informática se refiere al conjunto de derechos y libertades que deben ser reconocidos y protegidos para cada individuo frente a posibles abusos o invasiones de privacidad en el ámbito digital. Esto implica garantizar la integridad y confidencialidad de los datos personales, así como el derecho a la privacidad y el control sobre la información propia en el entorno digital (Pérez, 2000).

- **Libertad Sexual:** La autonomía sexual es la capacidad que tiene una persona para tomar decisiones y ejercer control sobre su vida sexual, incluyendo la elección de prácticas sexuales, relaciones sexuales y expresión de la identidad de género de acuerdo a sus propios deseos y valores (Quiroga, 2018).

- **Sistema Informático:** “Un nodo es cualquier punto de conexión único o conjunto de conectores interconectados entre sí, que operan o algunos de sus componentes operan de manera computarizada para procesar datos de acuerdo con un programa específico”. (Lamperti, 2017)

- **Tecnología de la Información:** “Esta definición engloba todo lo relacionado con el ámbito informático, la electrónica y las telecomunicaciones. Los avances tecnológicos, como Internet, la comunicación móvil y los satélites, han generado cambios significativos en el entorno socioeconómico, afectando las interacciones sociales y económicas”. (Ortiz, 2012)

2.4. Formulación de hipótesis

2.4.1. Hipótesis general

- Existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

2.4.2. Hipótesis específicas

- Existe relación significativa entre el marco legal con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Existe relación significativa entre las tipologías de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Existe relación significativa entre la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Existe relación significativa entre el incremento de la ciberdelincuencia con delitos informáticos en la provincia de Coronel Portillo 2023.

2.5. Variables

2.5.1. Variable 1

- Ciberdelincuencia.

2.5.2. Variable 2

- Delitos informáticos.

2.5.3. Operacionalización de las variables

- Se describe en la siguiente tabla:

Tabla 1

Operacionalización de las variables

Variable	Dimensiones	Indicadores	Escalas de medición
Ciberdelincuencia	• Marco legal • Tipologías • Seguridad publica • Incremento	• Tasa delictiva • Impacto económico • Vulnerabilidad digital • Respuesta legal • Nivel de riesgo • Percepción seguridad • Impacto económico • Frecuencia de delitos • Vulnerabilidades detectadas • Respuestas ante incidentes • Resiliencias frente ataques • Eficacia medidas de seguridad	Nunca Casi nunca A veces Casi siempre Siempre
Delitos informáticos	• Propiedad intelectual • Confidencialidad • Seguridad informática • Administración pública	• Tasa de Hurto • Pérdida económica • Víctimas financieras • Fraude digital • Transacciones sospechosas • Acceso no autorizado • Actividad anómala • Manipulación de datos • Correos electrónicos falsos • Páginas web fraudulentas • Phishing bancario • Malware engañoso • Acceso no autorizado • Transferencia indebida • Eliminación maliciosa • Manipulación ilegal	Nunca Casi nunca A veces Casi siempre Siempre

CAPÍTULO III

METODOLOGÍA

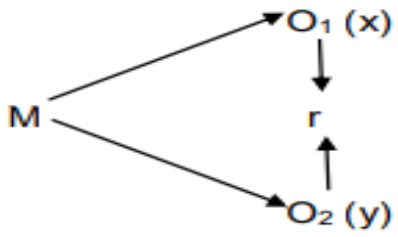
3.1. Diseño de la investigación

En primer lugar, se optó por un diseño de investigación de carácter descriptivo**,** dado que este permitió detallar con amplitud la realidad observada. A través del método de análisis, se procedió a caracterizar el objeto de estudio, identificando sus atributos y propiedades esenciales. De esta manera, la metodología empleada facilitó la organización, agrupación y sistematización de los elementos recolectados, lo cual contribuyó a alcanzar una comprensión más integral del fenómeno analizado (Baena, 2017).

Asimismo, la investigación se enmarcó dentro de un diseño no experimental**,** de tipo causal correlacional, lo que posibilitó examinar la relación existente entre las variables sin manipularlas directamente.

Figura 1

Esquema de la investigación



Donde:

M : Muestra utilizada para la aplicación de encuestas.

VO1 (x) : Ciberdelincuencia.

VO2 (y) : Delitos informáticos.

r : Relación.

Por otro lado, el ámbito de estudio correspondió al distrito fiscal de Ucayali, específicamente en la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo. En este escenario se llevó a cabo el análisis de las variables planteadas, con el fin de responder a los objetivos de investigación.

3.2. Población y muestra

3.2.1. Población

La población del estudio estuvo constituida por:

- **Treinta (30) Carpetas fiscales** que se encontraban en la etapa de investigación preparatoria por la comisión del delito de ciberdelincuencia en la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo.
- **Diez (10) Fiscales** pertenecientes a la misma institución.
- **Dos mil quinientos ochenta (2 580) abogados litigantes** que ejercían en dicha jurisdicción.

3.2.2. Muestra

La muestra se delimitó de la siguiente manera:

- **Veinte (20) Carpetas fiscales** correspondientes a investigaciones preparatorias por ciberdelincuencia en la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo.
- **Diez (10) Fiscales** de la misma institución.
- **Cincuenta (50) abogados litigantes** seleccionados de entre el total de profesionales de la jurisdicción.

3.3. Técnicas e instrumentos de recolección de datos

Para la obtención de la información se emplearon las siguientes técnicas e instrumentos:

- **Ficha de análisis documental:** Este instrumento se aplicó a veinte (20) carpetas fiscales que se encontraban en la etapa de investigación preparatoria por la comisión del delito de ciberdelincuencia en la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo. Su aplicación permitió recopilar, organizar y sistematizar la información contenida en los expedientes, garantizando un análisis riguroso de los casos seleccionados.

- **Encuesta:** Esta técnica se aplicó a diez (10) fiscales de la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo y a cincuenta (50) abogados litigantes. El cuestionario diseñado permitió obtener percepciones, opiniones y valoraciones relacionadas con las

variables de estudio, complementando la información documental con la perspectiva de los actores jurídicos involucrados.

Validez y confiabilidad del instrumento

El cuestionario fue sometido a un juicio de expertos**,** quienes evaluaron la pertinencia, claridad y coherencia de cada ítem en función de los objetivos de la investigación.

Para determinar la confiabilidad, se aplicó el coeficiente Alfa de Cronbach**,** obteniéndose un valor superior a 0,80, lo cual indicó una alta consistencia interna del instrumento. Este procedimiento aseguró que la encuesta fuera válida, confiable y adecuada para la recolección de los datos.

3.4. Técnicas para el procesamiento de la información

Una vez recolectada la información, los datos fueron organizados, codificados y sistematizados con la finalidad de garantizar su adecuada interpretación. Para ello se utilizaron diversos procedimientos que permitieron consolidar la información obtenida de las fuentes documentales y de campo.

En primer lugar, se recurrió a la aplicación del cuestionario, los cuales posibilitaron la recopilación de percepciones y valoraciones de fiscales y abogados litigantes. Paralelamente, se efectuó la evaluación de las actividades desarrolladas, lo que permitió registrar de manera detallada el contexto y dinámica de las acciones vinculadas al objeto de estudio.

Asimismo, se emplearon fichas técnicas de estadística, que facilitaron la tabulación ordenada de la información recolectada, así como el fichaje durante el estudio, acompañado de un exhaustivo análisis bibliográfico y documental, lo que contribuyó a sustentar teóricamente los hallazgos.

Para el procesamiento estadístico, los datos fueron ingresados al programa Statistical Package for the Social Sciences (SPSS), versión 27, el cual permitió aplicar tanto procedimientos descriptivos como inferenciales. En la primera etapa, se elaboraron tablas de frecuencias, porcentajes y medidas de tendencia central con el propósito de caracterizar a la muestra. En la segunda etapa, se aplicaron pruebas de correlación de Pearson, con la finalidad de determinar la relación existente entre las variables *ciberdelincuencia* y *delitos informáticos*.

Finalmente, los resultados obtenidos fueron organizados y presentados en tablas y figuras, elaboradas conforme a los lineamientos de la norma APA (7.ª edición), lo que favoreció una interpretación clara, coherente y rigurosa de la información.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Tabla 2

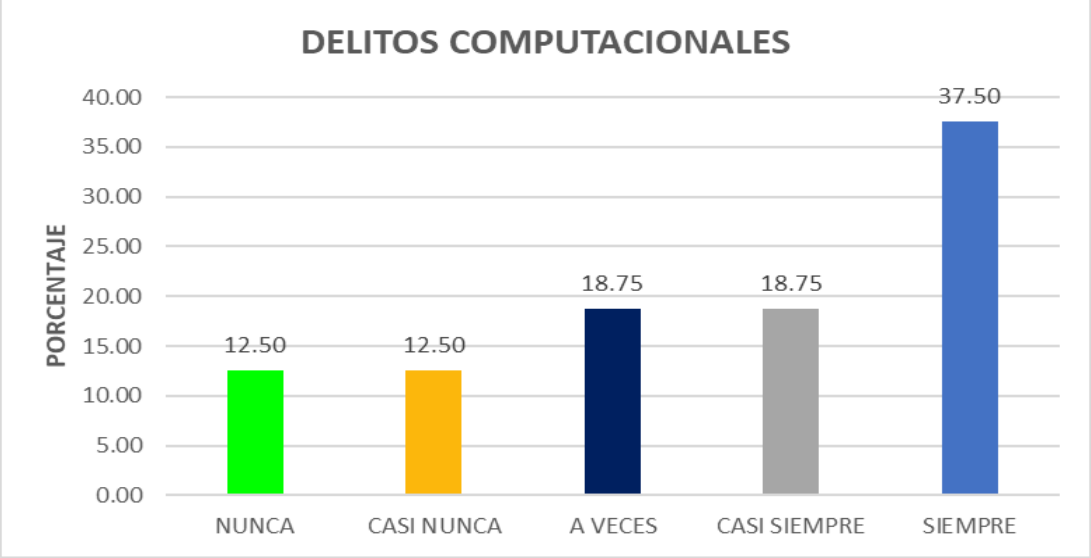
Dimensión Delitos Computacionales

	f	Porcentaje
NUNCA	10	12.50
CASI NUNCA	10	12.50
A VECES	15	18.75
CASI SIEMPRE	15	18.75
SIEMPRE	30	37.50
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 2

Dimensión Delitos Computacionales



Fuente: Tabla 2.

De la tabla y figura se observa que nunca se presentaron casos de Delitos de computación con respecto a la variable de Ciberdelincuencia con un 12.50%, casi nunca se presentaron casos de Delitos de computación con

respecto a la variable de Ciberdelincuencia con un 12.50%, a veces se presentaron casos de Delitos de computación con respecto a la variable de Ciberdelincuencia con un 18.75%, casi siempre se presentaron casos de Delitos de computación con respecto a la variable de Ciberdelincuencia con un 18.75%, siempre se presentaron casos de Delitos de computación con respecto a la variable de Ciberdelincuencia con un 37.50%.

Tabla 3

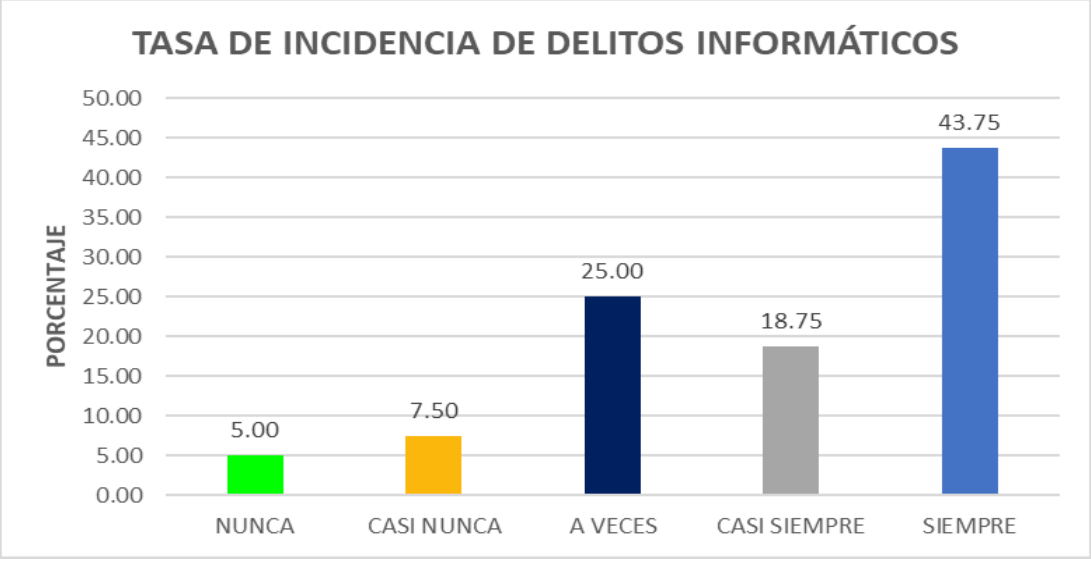
Dimensión Tasa de incidencia de delitos informáticos

	f	Porcentaje
NUNCA	4	5.00
CASI NUNCA	6	7.50
A VECES	20	25.00
CASI SIEMPRE	15	18.75
SIEMPRE	35	43.75
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 3

Dimensión tasa de incidencia de delitos informáticos



Fuente: Tabla 3.

De la tabla y figura, se observa que nunca se presentaron casos de Tasa de Incidencia de delitos informáticos con respecto a la variable Ciberdelincuencia con un 5.00%, casi nunca se presentaron casos de Tasa de Incidencia de delitos informáticos con respecto a la variable Ciberdelincuencia con un 7.50%, a veces se presentaron casos de Tasa de Incidencia de delitos informáticos con respecto a la variable Ciberdelincuencia con un 25.00%. casi siempre se presentaron casos de Tasa de Incidencia de delitos informáticos con respecto a la variable Ciberdelincuencia con un 18.75%, siempre se presentaron casos de Tasa de Incidencia de delitos informáticos con respecto a la variable Ciberdelincuencia con un 43.75%.

Tabla 4

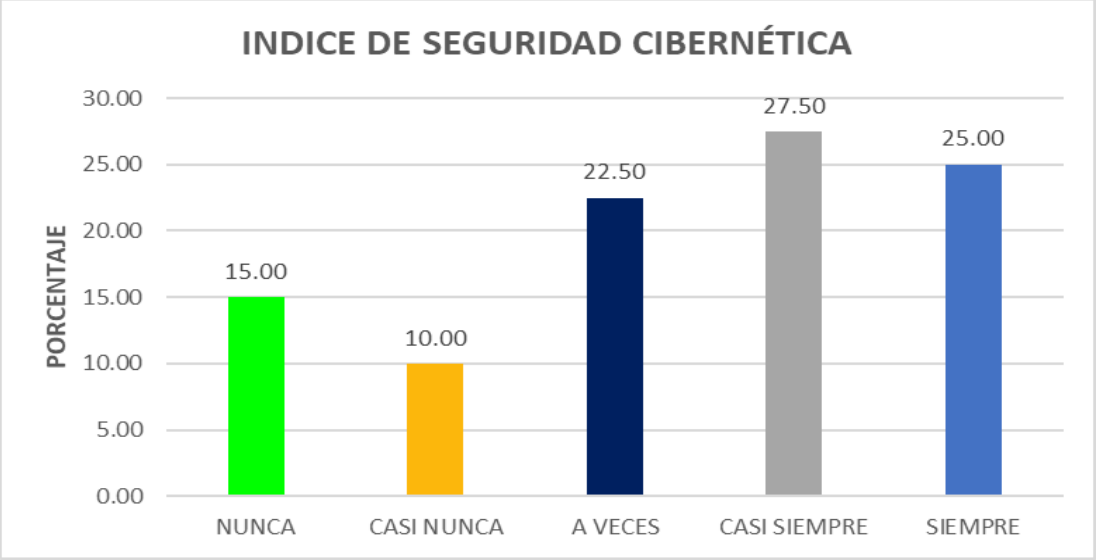
Dimensión índice de seguridad cibernética

	f	Porcentaje
NUNCA	12	15.00
CASI NUNCA	8	10.00
A VECES	18	22.50
CASI SIEMPRE	22	27.50
SIEMPRE	20	25.00
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 4

Dimensión índice de seguridad cibernética



Fuente: Tabla 4.

De la tabla y figura, se observa que nunca se presentaron casos de Índice de seguridad cibernética con respecto a la variable Ciberdelincuencia con 15.00%, casi nunca se presentaron casos de Índice de seguridad cibernética con respecto a la variable Ciberdelincuencia con 10.00%, a veces se presentaron casos de Índice de seguridad cibernética con respecto a la variable Ciberdelincuencia con 22.50%, casi siempre se presentaron casos de Índice de seguridad cibernética con respecto a la variable Ciberdelincuencia con 27.50%, siempre se presentaron casos de Índice de seguridad cibernética con respecto a la variable Ciberdelincuencia con 25.00%.

Tabla 5

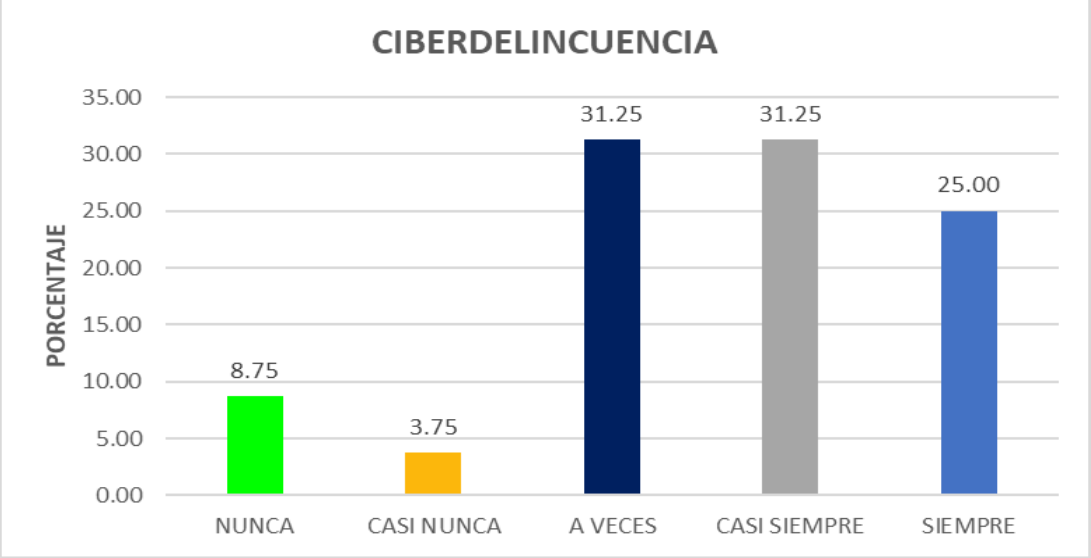
Variable Ciberdelincuencia

	f	Porcentaje
NUNCA	7	8.75
CASI NUNCA	3	3.75
A VECES	25	31.25
CASI SIEMPRE	25	31.25
SIEMPRE	20	25.00
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 5

Variable Ciberdelincuencia



Fuente: Tabla 5.

De la tabla y figura, se observa que nunca se presentaron casos con respecto a la variable Ciberdelincuencia con un 8.75%, casi nunca se presentaron casos con respecto a la variable Ciberdelincuencia con un 3.75%, a veces se presentaron casos con respecto a la variable Ciberdelincuencia con un 31.25%, casi siempre se presentaron casos con respecto a la variable Ciberdelincuencia con un 31.25%, siempre se presentaron casos con respecto a la variable Ciberdelincuencia con un 25.00%.

Tabla 6

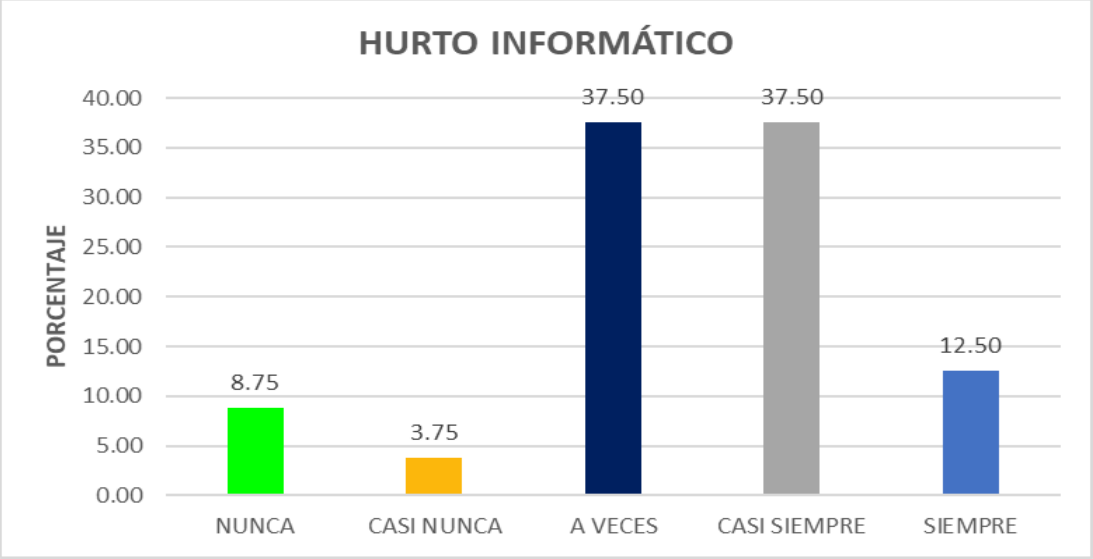
Dimensión Hurto Informático

	f	Porcentaje
NUNCA	7	8.75
CASI NUNCA	3	3.75
A VECES	30	37.50
CASI SIEMPRE	30	37.50
SIEMPRE	10	12.50
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 6

Dimensiones hurto informático



Fuente: Tabla 6.

De la tabla y figura, se observa que nunca se presentaron casos de hurto informático con respecto a la variable de Delitos informáticos con un 8.75%, casi nunca se presentaron casos de Hurto Informático con respecto a la variable de Delitos informáticos con un 3.75%, a veces se presentaron casos de Hurto Informático con respecto a la variable de Delitos informáticos con un 37.50%, casi siempre se presentaron casos de hurto Informático con

respecto a la variable de Delitos informáticos con un 37.50%, siempre se presentaron casos de hurto Informático con respecto a la variable de Delitos informáticos con un 12.50%.

Tabla 7

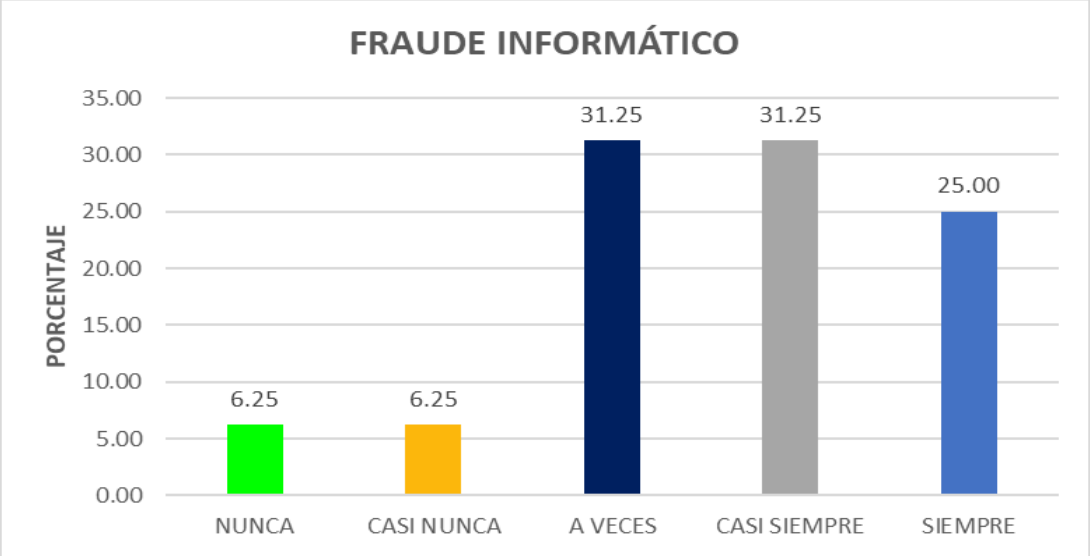
Dimensión fraude informático

	f	Porcentaje
NUNCA	5	6.25
CASI NUNCA	5	6.25
A VECES	25	31.25
CASI SIEMPRE	25	31.25
SIEMPRE	20	25.00
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 7

Dimensión fraude informático



Fuente: Tabla 7.

De la tabla y figura, se observa que nunca se presentaron casos de Fraude informático con respecto a la variable de Delitos informáticos con un 6.25%, casi nunca se presentaron casos de Fraude informático con respecto

a la variable de Delitos informáticos con un 6.25%, a veces se presentaron casos de Fraude informático con respecto a la variable de Delitos informáticos con un 31.25%, casi siempre se presentaron casos de Fraude informático con respecto a la variable de Delitos informáticos con un 31.25%. siempre se presentaron casos de Fraude informático con respecto a la variable de Delitos informáticos con un 25.00%.

Tabla 8

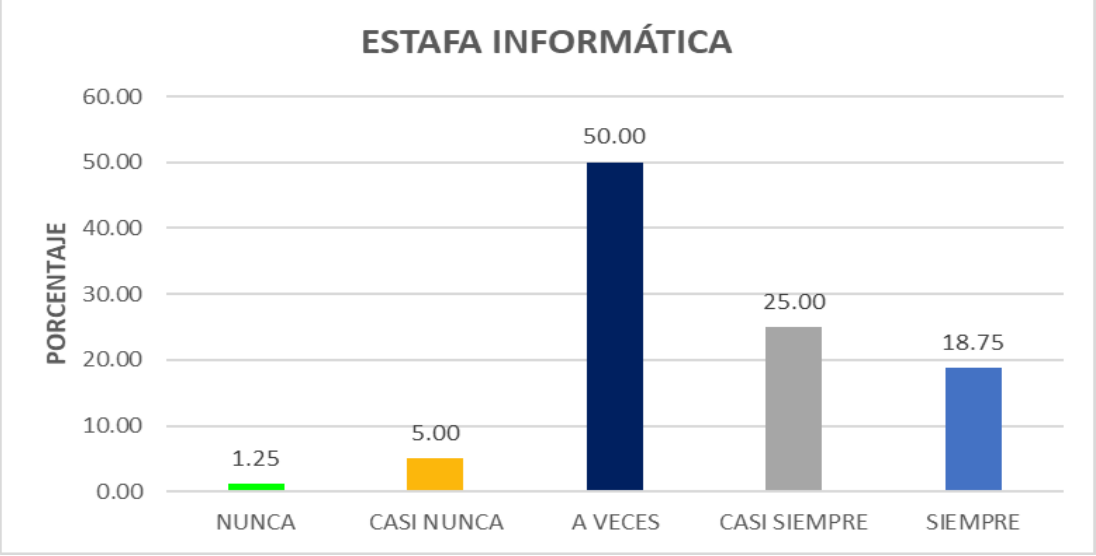
Dimensión Estafa informática

	f	Porcentaje
NUNCA	1	1.25
CASI NUNCA	4	5.00
A VECES	40	50.00
CASI SIEMPRE	20	25.00
SIEMPRE	15	18.75
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 8

Dimensión Estafa informática



Fuente: Tabla 8.

De la tabla y figura, se observa que nunca se presentaron casos de Estafa Informática con respecto a la variable de Delitos Informáticos con un 1.25%, casi nunca se presentaron casos de Estafa Informática con respecto a la variable de Delitos Informáticos con un 5.00%, a veces se presentaron casos de Estafa Informática con respecto a la variable de Delitos Informáticos con un 50.00%, casi siempre se presentaron casos de Estafa Informática con respecto a la variable de Delitos Informáticos con un 25.00%, siempre se presentaron casos de Estafa Informática con respecto a la variable de Delitos Informáticos con un 18.75%.

Tabla 9

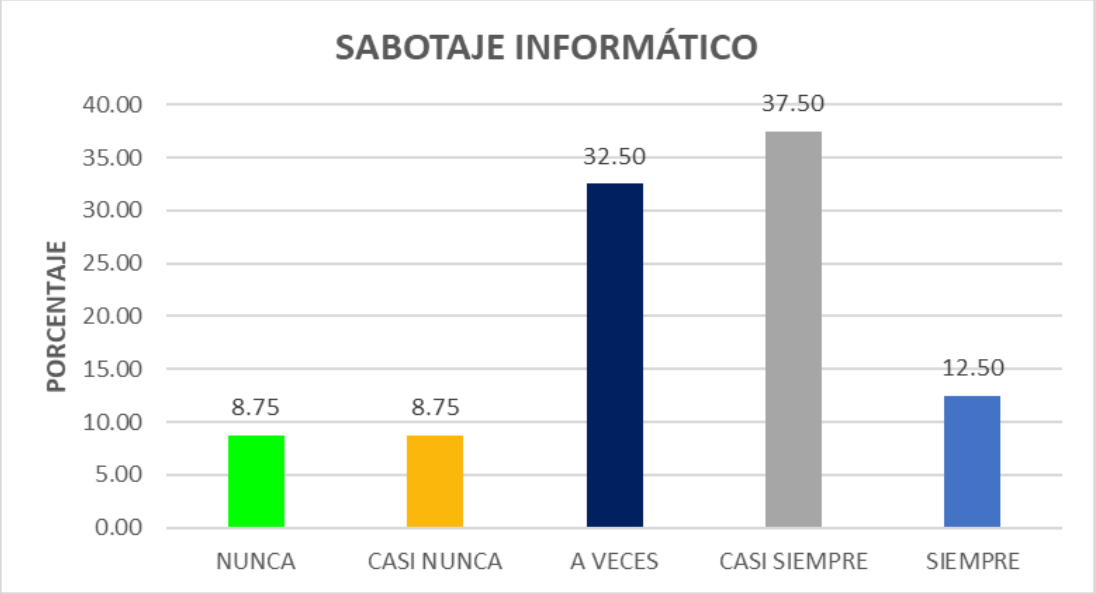
Dimensión Sabotaje Informático

	f	Porcentaje
NUNCA	7	8.75
CASI NUNCA	7	8.75
A VECES	26	32.50
CASI SIEMPRE	30	37.50
SIEMPRE	10	12.50
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 9

Dimensión Sabotaje informático



Fuente: Tabla 9.

De la tabla y figura, se observa que nunca se presentaron casos de Sabotaje Informático con respecto a la variable de Delitos informáticos con un 8.75%, casi nunca se presentaron casos de Sabotaje Informático con respecto a la variable de Delitos informáticos con un 8.75%, a veces se presentaron casos de Sabotaje Informático con respecto a la variable de Delitos informáticos con un 32.50%, casi siempre se presentaron casos de Sabotaje Informático con respecto a la variable de Delitos informáticos con un 37.50%, siempre se presentaron casos de Sabotaje Informático con respecto a la variable de Delitos informáticos con un 12.50%.

Tabla 10

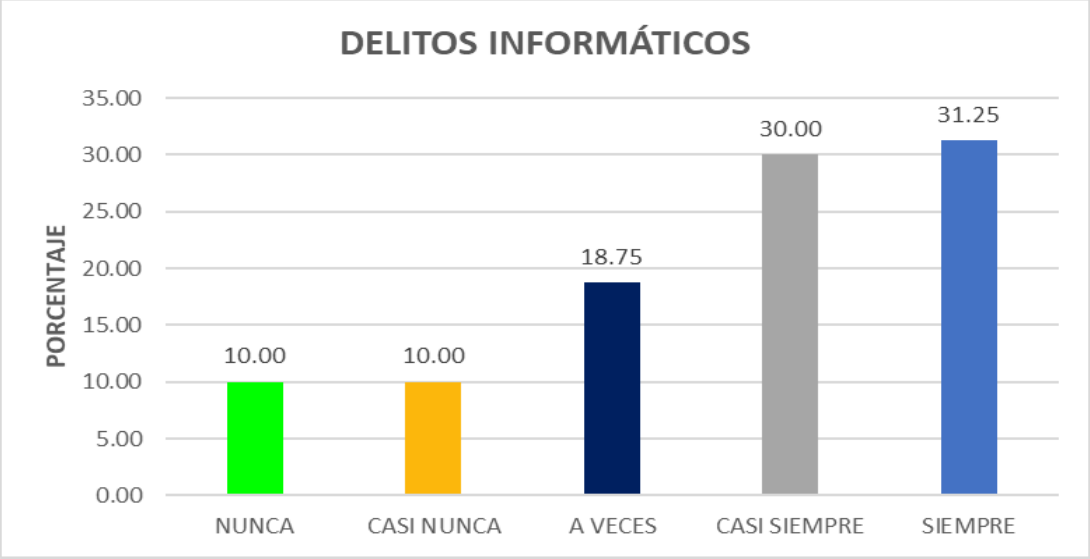
Variable Delitos informáticos

	f	Porcentaje
NUNCA	8	10.00
CASI NUNCA	8	10.00
A VECES	15	18.75
CASI SIEMPRE	24	30.00
SIEMPRE	25	31.25
TOTAL	80	100.00

Fuente: Instrumento aplicado.

Figura 10

Variable Delitos informáticos



Fuente: Tabla 10.

De la tabla y figura, se observa que nunca se prestaron casos con respecto a la variable de Delitos Informáticos con un 10.00%, casi nunca se prestaron casos con respecto a la variable de Delitos Informáticos con un 10.00%, a veces se prestaron casos con respecto a la variable de Delitos Informáticos con un 18.57%, casi siempre se prestaron casos con respecto a la variable de Delitos Informáticos con un 30.00%, siempre se prestaron casos con respecto a la variable de Delitos Informáticos con un 31.25%.

4.2. Prueba de hipótesis

4.2.1. Hipótesis general

- Ho: Existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.
- Hi: No existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Tabla 11

Existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023

Variable			Ciberdelincuencia	Delitos informáticos
Rho de Spearman	Ciberdelincuencia	Coeficiente de correlación	1000	,855**
		Sig. (bilateral)		,000
		N	80	80
	Delitos informáticos	Coeficiente de correlación	,855**	1000
		Sig. (bilateral)	,000	
		N	80	80

En la tabla, se observa que al contrastar la variable 1 Ciberdelincuencia y la variable 2 Delitos informáticos, se obtiene un coeficiente Rho de Spearman de 0.855 con p-valor = 000 (sig. bilateral) siendo una correlación positiva, por lo que se acepta la hipótesis planteada de la investigación. En conclusión, existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

4.2.2. Hipótesis específica 1

- Ho: Existe relación significativa entre el marco legal de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.
- Hi: No existe relación significativa entre el panorama actual de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Tabla 12

Existe relación entre el panorama actual de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023

Variable			Marco legal	Delitos Informáticos
Rho de Spearman	Marco legal	Coeficiente de correlación	1000	,864**
		Sig. (bilateral)		,000
		N	80	80
	Delitos informáticos	Coeficiente de correlación	,864**	
		Sig. (bilateral)	,000	1000
		N	80	80

En la tabla, se observa que al contrastar la dimensión marco legal y la variable 02 delitos informáticos, se obtiene un coeficiente Rho de Spearman de 0.864 con p-valor = 000 (sig. bilateral) siendo una correlación positiva, por lo que se acepta la hipótesis planteada de la investigación. En conclusión, existe relación significativa entre el marco legal de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

4.2.3. Hipótesis específica 2

- Ho: Existe relación significativa entre las tipologías de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Hi: No Existe relación significativa entre las tipologías de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.

Tabla 13

Existe relación significativa entre las tipologías de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023

Variable			Tipología	Delitos informáticos
Rho de Spearman	Tipología	Coeficiente de correlación	1000	,877**
		Sig. (bilateral)		,000
		N	80	80
	Delitos informáticos	Coeficiente de correlación	,877**	1000
		Sig. (bilateral)	,000	
		N	80	80

En la tabla, se observa que al contrastar la dimensión tipologías de ciberdelincuencia y la variable 02 delitos informáticos, se obtiene un coeficiente Rho de Spearman de 0.877 con p-valor = 000 (sig. bilateral) siendo una correlación positiva, por lo que se acepta la hipótesis planteada de la investigación. En conclusión, existe relación significativa entre las tipologías

de ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.

4.2.4. Hipótesis específica 3

- Ho: Existe relación significativa entre en la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Hi: No existe relación significativa entre en la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023.

Tabla 14

Existe relación significativa entre en la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023

Variable			Seguridad Pública	Delitos informáticos
Rho de Spearman	Seguridad pública	Coeficiente de correlación	1000	,847**
		Sig. (bilateral)		,000
		N	80	80
	delitos informáticos	Coeficiente de correlación	,847**	1000
		Sig. (bilateral)	,000	
		N	80	80

En la tabla, se observa que al contrastar la dimensión seguridad pública y la variable 2 delitos informáticos, se obtiene un coeficiente Rho de Spearman de 0.847 con p-valor = 000 (sig. bilateral) siendo una correlación positiva, por lo que se acepta la hipótesis planteada de la investigación. En conclusión,

existe relación significativa entre en la seguridad pública con los delitos informáticos en la provincia de Coronel Portillo 2023.

4.2.5. Hipótesis específica 4

- Ho: Existe relación entre el incremento de la ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.
- Hi: No existe relación entre el incremento de la ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.

Tabla 15

Existe relación entre el incremento de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023

Variable			Incremento	Delitos informáticos
Rho de Spearman	Incremento	Coeficiente de correlación	1000	,884**
		Sig. (bilateral)		,000
		N	80	80
	Delitos informáticos	Coeficiente de correlación	,884**	1000
		Sig. (bilateral)	,000	
		N	80	80

En la tabla, se observa que al contrastar la dimensión incremento de la ciberdelincuencia y la variable 2 Delitos informáticos, se obtiene un coeficiente Rho de Spearman de 0.884 con p-valor = 000 (sig. bilateral) siendo una correlación positiva, por lo que se acepta la hipótesis planteada de la

investigación. En conclusión, existe relación entre el incremento de la ciberdelincuencia con los delitos informáticos en la provincia de Coronel Portillo 2023.

4.3. Discusión de resultados

Los resultados obtenidos en la Dimensión Delitos Computacionales muestran una distribución variada en la frecuencia de ocurrencia de este fenómeno en la provincia de Coronel Portillo durante el año 2023. De acuerdo con la Tabla y Figura 2, se observó que en el 12.50% de los casos nunca se presentaron delitos de computación relacionados con la ciberdelincuencia, mientras que un porcentaje igual (12.50%) indicó que estos casos casi nunca ocurrieron. Sin embargo, se encontró que el 18.75% de los encuestados reportó que estos delitos ocurrieron "a veces", un 18.75% mencionó que "casi siempre" estuvieron presentes, y un 37.50% indicó que "siempre" se presentaron casos de delitos de computación en relación con la variable ciberdelincuencia.

Estos hallazgos reflejan una realidad preocupante respecto a la incidencia de los delitos computacionales en el contexto local, especialmente si se contrastan con estudios previos realizados a nivel nacional e internacional. En el ámbito internacional, la investigación de Zamora (2011) destaca que la criminalidad informática ha encontrado en los recursos económicos una vía para perpetrar delitos digitales, lo que se alinea con el aumento de casos registrados en Coronel Portillo. La dificultad para rastrear

a los perpetradores y la falta de marcos normativos actualizados, como se evidenció en Guatemala, también podrían ser factores que expliquen la prevalencia de estos delitos en la región.

Por otro lado, Tornel (2022) resalta que la Unión Europea ha intentado abordar la ciberdelincuencia con medidas específicas, pero la falta de una legislación unificada sigue siendo un desafío. En este sentido, la situación en Coronel Portillo parece reflejar esta misma problemática, ya que, a pesar de la existencia de normativas nacionales como la Ley Nº 30096, su aplicación enfrenta dificultades debido a vacíos legales y a la falta de recursos para su implementación efectiva (Carbajal, 2022).

A nivel nacional, la investigación de Chiriboga (2021) indica que la ciberdelincuencia no solo está asociada a fraudes financieros o ataques informáticos, sino que también afecta áreas como la libertad sexual, con un aumento en delitos como el acoso y la extorsión digital. Si bien los resultados en la provincia de Coronel Portillo no especifican la tipología exacta de los delitos computacionales reportados, la frecuencia con la que ocurren sugiere que es un problema estructural que requiere una mayor intervención de las autoridades.

Asimismo, Ventura (2021) enfatiza la falta de tipificación de modalidades específicas de ciberdelitos como el phishing, smishing y vishing en el sistema penal peruano. Este vacío normativo podría explicar por qué un porcentaje significativo de los encuestados en este estudio percibe que los delitos computacionales son una constante en su entorno. La ausencia de una

regulación clara y la escasez de recursos para la persecución efectiva de estos delitos pueden generar una percepción de impunidad y, en consecuencia, incentivar su incremento.

En la investigación local, Díaz y Huamán (2022) encontraron una correlación significativa entre el lavado de dinero y las actividades delictivas vinculadas a la ciberdelincuencia en la provincia de Coronel Portillo. Esto sugiere que los delitos computacionales pueden no ser eventos aislados, sino parte de una estructura criminal más amplia que involucra múltiples formas de delincuencia organizada.

En conclusión, los resultados obtenidos en esta investigación muestran que los delitos computacionales son un fenómeno recurrente en la provincia de Coronel Portillo, con un 37.50% de los encuestados indicando que siempre se presentan casos en relación con la ciberdelincuencia. Esta tendencia es consistente con los hallazgos de estudios previos tanto a nivel nacional como internacional, los cuales resaltan la falta de una legislación adecuada, la carencia de recursos para su persecución y la creciente sofisticación de los ciberdelincuentes como factores determinantes en la prevalencia de estos delitos. La necesidad de fortalecer la legislación y mejorar la capacitación de las autoridades en ciberseguridad es una prioridad para mitigar esta problemática en el contexto local.

Los resultados obtenidos en la Dimensión Tasa de Incidencia de Delitos Informáticos reflejan una preocupante tendencia en la provincia de Coronel Portillo durante el año 2023. A partir de la Tabla y Figura 3, se observa que en

el 5.00% de los casos nunca se presentaron delitos informáticos en relación con la ciberdelincuencia, mientras que un 7.50% indicó que estos casos casi nunca ocurrieron. No obstante, el 25.00% de los encuestados reportó que estos delitos ocurrieron "a veces", un 18.75% mencionó que "casi siempre" estuvieron presentes, y un 43.75% indicó que "siempre" se presentaron casos de delitos informáticos relacionados con la ciberdelincuencia.

Estos hallazgos evidencian la creciente incidencia de delitos informáticos en la región, lo que concuerda con estudios previos realizados a nivel nacional e internacional. En el ámbito internacional, Zamora (2011) resalta cómo la criminalidad informática ha evolucionado, convirtiéndose en una amenaza de difícil rastreo debido a la naturaleza transfronteriza de estos delitos. La situación en Guatemala, donde la legislación desactualizada genera un vacío legal, es similar a la que enfrenta la provincia de Coronel Portillo, donde la respuesta institucional ante los delitos informáticos todavía es insuficiente.

Por otro lado, Tornel (2022) destaca que la Unión Europea y España han trabajado en fortalecer la normativa contra la ciberdelincuencia, pero aún persisten obstáculos relacionados con la falta de definiciones claras y dificultades en la obtención de pruebas digitales. En este sentido, el alto porcentaje de incidencia en Coronel Portillo puede estar relacionado con la carencia de herramientas legales y técnicas para la detección y persecución de estos delitos.

A nivel nacional, Carbajal (2022) señala que el fraude informático es una de las modalidades más recurrentes de delitos informáticos en el Perú. Sin embargo, muchas de estas prácticas no están tipificadas en la Ley N.º 30096, lo que dificulta su sanción. Este vacío legal podría ser una de las razones por las cuales los delitos informáticos muestran una alta tasa de incidencia en la provincia de Coronel Portillo, ya que los delincuentes pueden operar con una sensación de impunidad.

En relación con la criminalidad organizada, Díaz y Huamán (2022) encontraron una correlación significativa entre el lavado de dinero y el uso de criptomonedas para actividades ilícitas en Coronel Portillo. Este hallazgo sugiere que los delitos informáticos no solo afectan a usuarios individuales, sino que también pueden estar vinculados a redes delictivas más amplias, lo que explicaría la alta frecuencia con la que estos delitos se reportan en la provincia.

Asimismo, Ventura (2021) resalta que modalidades como el phishing, smishing y vishing no están adecuadamente reguladas en el sistema penal peruano, lo que permite que estos delitos prosperen sin una persecución efectiva. Esta falta de regulación podría explicar por qué un porcentaje significativo de la población encuestada en Coronel Portillo percibe que los delitos informáticos son recurrentes.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que el delito informático afecta directamente las operaciones financieras en los bancos de Coronel Portillo, generando una vulnerabilidad significativa en el

sector bancario. El alto porcentaje de encuestados que señala la constante presencia de estos delitos sugiere que esta problemática no se limita al ámbito financiero, sino que tiene un impacto generalizado en distintos sectores.

En conclusión, la Dimensión Tasa de Incidencia de Delitos Informáticos muestra que la ciberdelincuencia es un problema constante en la provincia de Coronel Portillo, con un 43.75% de los encuestados indicando que estos delitos "siempre" están presentes. La comparación con estudios previos revela que esta problemática se ve agravada por la falta de actualización legislativa, la impunidad en la persecución de estos delitos y la creciente sofisticación de los ciberdelincuentes. Para reducir esta alta incidencia, es fundamental fortalecer el marco normativo, mejorar la capacitación de las autoridades en ciberseguridad y fomentar estrategias de cooperación internacional.

Los resultados obtenidos en la Dimensión Índice de Seguridad Cibernética muestran una variabilidad en la percepción de la seguridad digital en la provincia de Coronel Portillo durante el año 2023. De acuerdo con la Tabla y Figura 4, se observó que el 15.00% de los encuestados indicaron que nunca se presentaron casos relacionados con el Índice de Seguridad Cibernética en relación con la ciberdelincuencia, mientras que el 10.00% señaló que estos casos "casi nunca" ocurrieron. Sin embargo, un 22.50% afirmó que estos eventos sucedieron "a veces", un 27.50% mencionó que "casi siempre" estuvieron presentes, y un 25.00% indicó que "siempre" se presentaron casos en esta dimensión.

Estos hallazgos evidencian una percepción ambivalente sobre la seguridad cibernética en la región, lo que se alinea con estudios previos realizados tanto a nivel nacional como internacional. En el ámbito internacional, Zamora (2011) destaca que la criminalidad informática ha evolucionado y ha encontrado en las tecnologías digitales una herramienta para perpetrar delitos que resultan difíciles de rastrear. La situación en Guatemala, donde la legislación desactualizada dificulta la persecución de delitos cibernéticos, es similar a la de Coronel Portillo, donde la percepción de seguridad cibernética es fluctuante debido a la falta de mecanismos de control y prevención eficaces.

Por otro lado, Tornel (2022) resalta que la Unión Europea ha intentado abordar la ciberdelincuencia mediante el fortalecimiento de normativas, pero la falta de uniformidad en la legislación y las dificultades en la obtención de pruebas digitales han limitado la efectividad de estas medidas. Esto se refleja en los resultados obtenidos en Coronel Portillo, donde un porcentaje considerable de la población percibe que la seguridad cibernética no es constante ni adecuada.

A nivel nacional, Carbajal (2022) señala que la legislación peruana en materia de seguridad cibernética es insuficiente para enfrentar los crecientes desafíos de la ciberdelincuencia. La Ley Nº 30096, aunque representa un avance, no aborda de manera específica aspectos como el phishing, el smishing o el vishing, lo que deja vacíos legales significativos que afectan la percepción de seguridad en el entorno digital.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que la deficiencia en las medidas de seguridad cibernética afecta significativamente a las operaciones financieras en los bancos de Coronel Portillo. Esta vulnerabilidad en el sector bancario podría estar contribuyendo a la percepción de que la seguridad cibernética es deficiente en la región, lo que se refleja en el porcentaje de encuestados que reportan una alta frecuencia de incidentes.

Asimismo, Díaz y Huamán (2022) identificaron una relación significativa entre el lavado de dinero y el uso de criptomonedas en actividades delictivas dentro de la provincia. Esto indica que la falta de un marco regulatorio sólido no solo facilita la ciberdelincuencia, sino que también contribuye a la sensación de inseguridad digital entre los ciudadanos.

En conclusión, los resultados de esta investigación muestran que la percepción sobre el Índice de Seguridad Cibernética en Coronel Portillo está dividida, con un 27.50% de los encuestados afirmando que "casi siempre" existen problemas de seguridad cibernética y un 25.00% indicando que "siempre" están presentes. Esta tendencia se correlaciona con estudios previos que han evidenciado la falta de normativas actualizadas, la escasez de recursos tecnológicos y la creciente sofisticación de los ciberdelincuentes. Para mejorar la seguridad cibernética en la región, es fundamental fortalecer la legislación, promover una mayor capacitación en ciberseguridad y fomentar la colaboración entre entidades públicas y privadas en la lucha contra la ciberdelincuencia.

Los resultados obtenidos en relación con la Variable Ciberdelincuencia reflejan una tendencia preocupante en la provincia de Coronel Portillo durante el año 2023. De acuerdo con la Tabla y Figura 5, se observó que el 8.75% de los encuestados indicaron que nunca se presentaron casos de ciberdelincuencia, mientras que el 3.75% señaló que estos casos "casi nunca" ocurrieron. No obstante, un 31.25% afirmó que estos eventos sucedieron "a veces", un 31.25% mencionó que "casi siempre" estuvieron presentes, y un 25.00% indicó que "siempre" se presentaron casos de ciberdelincuencia.

Estos hallazgos evidencian que la ciberdelincuencia es una amenaza persistente en la región, lo que se alinea con estudios previos tanto a nivel nacional como internacional. En el ámbito internacional, Zamora (2011) destaca que la criminalidad informática se ha convertido en un problema transfronterizo, debido a la facilidad con la que los ciberdelincuentes operan en entornos digitales sin restricciones geográficas. En Guatemala, por ejemplo, la falta de legislación actualizada ha dificultado la persecución efectiva de estos delitos, lo que permite que los ciberdelincuentes actúen con impunidad. Este contexto es similar al de Coronel Portillo, donde la alta incidencia de ciberdelincuencia podría estar relacionada con vacíos normativos y la falta de herramientas para la identificación y sanción de los responsables.

Por otro lado, Tornel (2022) enfatiza que, en Europa, aunque existen esfuerzos para regular la ciberdelincuencia y mejorar la ciberseguridad, la falta de estándares unificados y la complejidad de la obtención de pruebas digitales

dificultan la eficacia de las acciones judiciales. En este sentido, los resultados obtenidos en Coronel Portillo reflejan una problemática similar, donde la aplicación de medidas legales y técnicas sigue siendo un desafío en la lucha contra la ciberdelincuencia.

A nivel nacional, Carbajal (2022) resalta que los delitos informáticos han aumentado en el Perú, especialmente en lo que respecta al fraude digital y la suplantación de identidad. No obstante, la Ley Nº 30096 no tipifica adecuadamente algunas modalidades emergentes de ciberdelincuencia, como el phishing y el smishing, lo que dificulta la persecución penal de estos delitos. Este vacío normativo podría estar contribuyendo a la percepción de que la ciberdelincuencia es un fenómeno recurrente en la provincia de Coronel Portillo, dado que la población no percibe respuestas contundentes por parte de las autoridades.

Asimismo, Chiriboga (2021) estudió la relación entre la ciberdelincuencia y el delito contra la libertad sexual en el Perú, encontrando que la facilidad con la que los delincuentes acceden a sus víctimas a través de plataformas digitales ha incrementado la cantidad de denuncias por acoso, extorsión y explotación en línea. Si bien los resultados de esta investigación no detallan la naturaleza de los delitos de ciberdelincuencia en Coronel Portillo, el alto porcentaje de encuestados que perciben su ocurrencia sugiere que estos delitos podrían abarcar una variedad de modalidades delictivas.

Desde una perspectiva local, Díaz y Huamán (2022) identificaron una fuerte relación entre el lavado de dinero y la ciberdelincuencia en la provincia

de Coronel Portillo, con un énfasis en el uso de criptomonedas para el movimiento de fondos ilícitos. Este hallazgo sugiere que la ciberdelincuencia en la región no solo afecta a ciudadanos individuales, sino que también puede estar vinculada a redes criminales más grandes, lo que explicaría la alta frecuencia con la que estos delitos son reportados.

De igual manera, Cataño y Panduro (2023) encontraron que el delito informático tiene un impacto directo en las operaciones financieras en los bancos de la provincia, con una correlación fuerte entre el aumento de fraudes digitales y la vulnerabilidad del sector bancario. Esto refuerza la idea de que la ciberdelincuencia no solo se manifiesta en delitos individuales, sino que afecta la estabilidad de sectores clave en la economía local.

En conclusión, los resultados de esta investigación muestran que la Variable Ciberdelincuencia es un fenómeno recurrente en la provincia de Coronel Portillo, con un 31.25% de los encuestados afirmando que estos delitos "casi siempre" ocurren y un 25.00% indicando que "siempre" están presentes. La comparación con estudios previos revela que esta tendencia está influenciada por factores como la falta de actualización normativa, la ausencia de recursos para la persecución de estos delitos y la creciente sofisticación de los ciberdelincuentes. Para enfrentar esta problemática, es esencial fortalecer el marco legal, mejorar la infraestructura tecnológica para la detección de delitos cibernéticos y fomentar la cooperación entre entidades nacionales e internacionales en la lucha contra la ciberdelincuencia.

Los resultados obtenidos en la Dimensión Hurto Informático reflejan una preocupante incidencia de este delito en la provincia de Coronel Portillo durante el año 2023. De acuerdo con la Tabla y Figura 6, se observó que el 8.75% de los encuestados indicaron que nunca se presentaron casos de hurto informático, mientras que el 3.75% señaló que estos casos "casi nunca" ocurrieron. No obstante, un 37.50% afirmó que estos eventos sucedieron "a veces", un porcentaje igual (37.50%) mencionó que "casi siempre" estuvieron presentes, y un 12.50% indicó que "siempre" se presentaron casos de hurto informático.

Estos resultados reflejan la persistente vulnerabilidad de la población ante este tipo de delito, lo que concuerda con estudios previos tanto a nivel nacional como internacional. En el ámbito internacional, Zamora (2011) destaca que la criminalidad informática ha encontrado en los recursos digitales una vía efectiva para perpetrar delitos como el hurto informático, aprovechando la evasividad que brindan las nuevas tecnologías. En Guatemala, por ejemplo, la falta de legislación actualizada ha permitido la proliferación de estos delitos, una problemática similar a la que enfrenta la provincia de Coronel Portillo, donde las normativas vigentes no parecen ser suficientes para mitigar estos actos delictivos.

Por otro lado, Tornel (2022) enfatiza que, en España y la Unión Europea, se han establecido medidas para mejorar la ciberseguridad y combatir delitos como el hurto informático. Sin embargo, la dificultad para identificar a los perpetradores y la falta de uniformidad en las regulaciones han

limitado la eficacia de estas estrategias. En este sentido, la percepción de que el hurto informático es frecuente en Coronel Portillo podría estar vinculada con estos mismos factores, dado que los delincuentes aprovechan la falta de un marco legal claro y las dificultades en la persecución penal de estos delitos.

A nivel nacional, Carbajal (2022) resalta que el fraude informático y el hurto de información digital han ido en aumento en el Perú, en parte debido a vacíos en la Ley Nº 30096, la cual no tipifica adecuadamente nuevas modalidades delictivas digitales. Este vacío normativo puede explicar la percepción de inseguridad digital en Coronel Portillo, donde un alto porcentaje de encuestados indica que el hurto informático ocurre con frecuencia.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que el hurto informático afecta directamente las operaciones financieras en los bancos de Coronel Portillo, generando vulnerabilidades significativas en el sector bancario. Esto sugiere que la alta incidencia de hurto informático en la región no solo se limita a usuarios individuales, sino que también compromete la estabilidad del sistema financiero, afectando la confianza en las transacciones digitales.

Asimismo, Díaz y Huamán (2022) identificaron una correlación entre el lavado de dinero y el uso de tecnologías digitales para la transferencia ilícita de fondos en la provincia de Coronel Portillo. Esto indica que el hurto informático no solo se da a nivel de usuarios comunes, sino que también podría formar parte de redes delictivas más amplias que buscan aprovechar las vulnerabilidades del sistema financiero digital.

En conclusión, los resultados de esta investigación muestran que la Dimensión Hurto Informático es un problema significativo en la provincia de Coronel Portillo, con un 37.50% de los encuestados afirmando que estos delitos ocurren "casi siempre" y otro 37.50% indicando que ocurren "a veces". Estos hallazgos coinciden con estudios previos que han evidenciado la falta de normativas actualizadas, la insuficiencia de recursos tecnológicos para la detección de estos delitos y la creciente sofisticación de los delincuentes informáticos. Para enfrentar esta problemática, es esencial fortalecer el marco legal, incrementar las medidas de seguridad digital y fomentar la educación en ciberseguridad para reducir la vulnerabilidad de la población frente a este tipo de delitos.

Los resultados obtenidos en la Dimensión Fraude Informático evidencian una problemática persistente en la provincia de Coronel Portillo durante el año 2023. Según la Tabla y Figura 7, el 6.25% de los encuestados indicaron que nunca se presentaron casos de fraude informático, mientras que un porcentaje igual (6.25%) señaló que estos casos "casi nunca" ocurrieron. Sin embargo, un 31.25% afirmó que estos eventos sucedieron "a veces", otro 31.25% mencionó que "casi siempre" estuvieron presentes, y un 25.00% indicó que "siempre" se presentaron casos de fraude informático en relación con los delitos informáticos.

Estos hallazgos demuestran que el fraude informático es un delito frecuente en la región, lo que concuerda con estudios previos a nivel nacional e internacional. En el ámbito internacional, Zamora (2011) destaca que la

criminalidad informática ha evolucionado y se ha convertido en un problema global, aprovechando la falta de regulación efectiva y los avances tecnológicos que facilitan la suplantación de identidad y el acceso no autorizado a sistemas financieros. En el caso de Guatemala, la ausencia de una legislación actualizada ha propiciado el incremento de fraudes informáticos, una realidad que parece replicarse en Coronel Portillo, donde los marcos regulatorios no han sido suficientemente eficaces para frenar esta modalidad delictiva.

Por otro lado, Tornel (2022) enfatiza que la Unión Europea ha trabajado en el fortalecimiento de normativas contra el fraude informático, pero la falta de armonización legislativa y la dificultad para rastrear transacciones fraudulentas continúan siendo desafíos relevantes. Este contexto es similar al peruano, donde los mecanismos de persecución del fraude informático aún presentan deficiencias, lo que contribuye a la percepción de que estos delitos ocurren con alta frecuencia.

A nivel nacional, Carbajal (2022) identifica al fraude informático como el delito de mayor incidencia en el Perú dentro de los delitos informáticos, destacando que modalidades como la clonación de tarjetas, compras fraudulentas en línea y transferencias de fondos no autorizadas han experimentado un incremento notable en los últimos años. Sin embargo, estas modalidades no están claramente tipificadas en la Ley Nº 30096, lo que dificulta su sanción y permite que los delincuentes continúen operando con impunidad. Este vacío legal podría ser un factor determinante en la alta

frecuencia con la que se reportan casos de fraude informático en Coronel Portillo.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que el fraude informático afecta de manera significativa a las operaciones financieras de los bancos en la provincia de Coronel Portillo. Este hallazgo sugiere que no solo los ciudadanos son víctimas de estos delitos, sino también las instituciones financieras, lo que agrava la percepción de inseguridad digital en la región. La falta de mecanismos efectivos de detección y prevención en los bancos locales podría estar contribuyendo a la persistencia de este problema.

Asimismo, Díaz y Huamán (2022) identificaron una correlación entre el fraude informático y el lavado de dinero en la provincia de Coronel Portillo, destacando el uso de criptomonedas y transacciones digitales como mecanismos para ocultar fondos ilícitos. Esto refuerza la idea de que el fraude informático no solo es un delito individual, sino que también puede formar parte de estructuras delictivas más amplias, lo que explica su constante presencia en la región.

En conclusión, los resultados de esta investigación indican que la Dimensión Fraude Informático es un problema relevante en la provincia de Coronel Portillo, con un 31.25% de los encuestados afirmando que estos delitos "casi siempre" ocurren y un 25.00% indicando que "siempre" están presentes. Estos hallazgos coinciden con investigaciones previas que han evidenciado la falta de normativas actualizadas, la insuficiencia de recursos

tecnológicos para la detección de estos delitos y la creciente sofisticación de los delincuentes informáticos. Para mitigar esta problemática, es necesario fortalecer la legislación, incrementar las medidas de seguridad en las instituciones financieras y promover la educación en ciberseguridad entre la población.

Los resultados obtenidos en la Dimensión Estafa Informática evidencian que este delito es una de las modalidades más recurrentes dentro de los delitos informáticos en la provincia de Coronel Portillo durante el año 2023. Según la Tabla y Figura 8, el 1.25% de los encuestados indicó que nunca se presentaron casos de estafa informática, mientras que el 5.00% señaló que estos casos "casi nunca" ocurrieron. Sin embargo, un 50.00% afirmó que estos eventos sucedieron "a veces", un 25.00% mencionó que "casi siempre" estuvieron presentes, y un 18.75% indicó que "siempre" se presentaron casos de estafa informática en relación con los delitos informáticos.

Estos resultados evidencian que la estafa informática es un problema constante y de alta frecuencia en la región, lo que concuerda con estudios previos tanto a nivel nacional como internacional. En el ámbito internacional, Zamora (2011) destaca que la criminalidad informática ha encontrado en el fraude y la estafa digital un mecanismo eficiente para la obtención ilícita de recursos, beneficiándose de la falta de regulación efectiva y de la dificultad para rastrear transacciones fraudulentas. En Guatemala, por ejemplo, la ausencia de legislación actualizada ha facilitado la proliferación de estos

delitos, una situación que parece replicarse en la provincia de Coronel Portillo, donde los ciudadanos perciben con frecuencia la ocurrencia de estafas digitales.

Por otro lado, Tornel (2022) enfatiza que la Unión Europea ha implementado normativas para combatir la estafa informática, pero las dificultades en la recopilación de pruebas digitales y la falta de mecanismos transfronterizos eficientes han limitado la persecución de estos delitos. En este sentido, el alto porcentaje de incidencia en Coronel Portillo podría estar relacionado con la carencia de marcos legales específicos y la dificultad de las instituciones locales para procesar este tipo de crímenes.

A nivel nacional, Carbajal (2022) identifica a la estafa informática como una de las modalidades más frecuentes de los delitos informáticos en el Perú, especialmente en fraudes relacionados con compras en línea, suplantación de identidad y engaños financieros. Sin embargo, la Ley Nº 30096 aún presenta vacíos en la tipificación de estas modalidades delictivas, lo que dificulta la sanción efectiva y permite que los ciberdelincuentes continúen operando sin mayores consecuencias legales. Esta falta de regulación clara podría estar contribuyendo a la percepción de que la estafa informática es un delito recurrente en Coronel Portillo.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que la estafa informática tiene un impacto significativo en las operaciones financieras en los bancos de la provincia de Coronel Portillo. Este hallazgo sugiere que los fraudes digitales no solo afectan a usuarios individuales, sino

que también comprometen la seguridad del sistema financiero local, lo que podría estar influyendo en la percepción de que estos delitos ocurren con frecuencia en la región.

Asimismo, Díaz y Huamán (2022) identificaron una relación entre la estafa informática y el lavado de dinero en la provincia de Coronel Portillo, destacando que los ciberdelincuentes utilizan diversas plataformas digitales y criptomonedas para ocultar sus operaciones fraudulentas. Este hallazgo refuerza la idea de que la estafa informática en la región no solo se limita a engaños individuales, sino que forma parte de esquemas delictivos más complejos.

En conclusión, los resultados de esta investigación muestran que la Dimensión Estafa Informática es una problemática relevante en la provincia de Coronel Portillo, con un 50.00% de los encuestados afirmando que estos delitos ocurren "a veces", un 25.00% indicando que ocurren "casi siempre" y un 18.75% señalando que "siempre" están presentes. Estos hallazgos coinciden con investigaciones previas que han señalado la falta de normativas actualizadas, la insuficiencia de recursos para la detección de estos delitos y la creciente sofisticación de los estafadores digitales. Para mitigar esta problemática, es fundamental fortalecer la legislación, incrementar la seguridad en las plataformas digitales y fomentar campañas de concienciación sobre los riesgos de la estafa informática entre la población.

Los resultados obtenidos en la Dimensión Sabotaje Informático reflejan una significativa presencia de este delito en la provincia de Coronel Portillo

durante el año 2023. Según la Tabla y Figura 9, el 8.75% de los encuestados indicó que nunca se presentaron casos de sabotaje informático, mientras que un porcentaje igual (8.75%) señaló que estos casos "casi nunca" ocurrieron. Sin embargo, un 32.50% afirmó que estos eventos sucedieron "a veces", un 37.50% mencionó que "casi siempre" estuvieron presentes, y un 12.50% indicó que "siempre" se presentaron casos de sabotaje informático.

Estos hallazgos evidencian que el sabotaje informático es un problema recurrente en la región, lo que coincide con estudios previos realizados tanto a nivel nacional como internacional. En el ámbito internacional, Zamora (2011) resalta que la criminalidad informática ha evolucionado, encontrando en las infraestructuras digitales un blanco para perpetrar ataques que afectan la estabilidad de sistemas de información críticos. En el caso de Guatemala, la falta de actualización legislativa ha dificultado la persecución de estos delitos, lo que permite que los ciberdelincuentes actúen con impunidad. Esta realidad podría reflejarse en Coronel Portillo, donde la percepción de la incidencia de sabotaje informático sugiere una deficiencia en la protección de los sistemas digitales.

Por otro lado, Tornel (2022) enfatiza que la Unión Europea ha implementado medidas para fortalecer la ciberseguridad y combatir delitos como el sabotaje informático. No obstante, las dificultades en la cooperación internacional y la falta de normativas homogéneas han limitado la efectividad de estas iniciativas. Este contexto es similar al de la provincia de Coronel Portillo, donde las instituciones locales aún enfrentan barreras tecnológicas y

legales para mitigar los ataques informáticos.

A nivel nacional, Carbajal (2022) señala que el sabotaje informático, aunque menos frecuente que otros delitos informáticos como el fraude y la estafa, representa una amenaza creciente para empresas y entidades gubernamentales. La Ley Nº 30096 no especifica con suficiente claridad las sanciones para este tipo de delitos, lo que genera dificultades en su judicialización y sanción. Esto podría explicar por qué un porcentaje considerable de los encuestados en Coronel Portillo percibe que estos delitos ocurren con frecuencia.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que el sabotaje informático afecta directamente la seguridad de las operaciones financieras en los bancos de la provincia de Coronel Portillo. Esto indica que los ciberdelincuentes no solo buscan obtener beneficios económicos mediante fraudes o robos, sino que también emplean tácticas de destrucción de datos o alteración de sistemas con fines estratégicos. La alta frecuencia de sabotaje informático reportada en la provincia podría estar vinculada a este tipo de ataques dirigidos contra infraestructuras clave.

Asimismo, Díaz y Huamán (2022) identificaron una correlación entre el sabotaje informático y el crimen organizado en Coronel Portillo, destacando que grupos delictivos utilizan ataques a sistemas digitales para desestabilizar instituciones y facilitar otras actividades ilícitas, como el lavado de dinero y la evasión fiscal. Este hallazgo refuerza la idea de que el sabotaje informático en la región no es un fenómeno aislado, sino que forma parte de estrategias

delictivas más amplias.

En conclusión, los resultados de esta investigación muestran que la Dimensión Sabotaje Informático es una preocupación significativa en la provincia de Coronel Portillo, con un 37.50% de los encuestados afirmando que estos delitos "casi siempre" ocurren y un 12.50% indicando que "siempre" están presentes. Estos hallazgos coinciden con estudios previos que han señalado la falta de regulaciones actualizadas, la insuficiencia de recursos tecnológicos y la creciente sofisticación de los ciberdelincuentes. Para mitigar esta problemática, es esencial fortalecer la legislación, mejorar la seguridad de las infraestructuras digitales y fomentar una mayor cooperación entre entidades gubernamentales y privadas para prevenir y responder a ataques de sabotaje informático.

Los resultados obtenidos en la Variable Delitos Informáticos reflejan una alta incidencia de este fenómeno en la provincia de Coronel Portillo durante el año 2023. Según la Tabla y Figura 10, el 10.00% de los encuestados indicaron que nunca se presentaron casos de delitos informáticos, mientras que un porcentaje igual (10.00%) señaló que estos casos "casi nunca" ocurrieron. Sin embargo, un 18.57% afirmó que estos delitos sucedieron "a veces", un 30.00% mencionó que "casi siempre" estuvieron presentes, y un 31.25% indicó que "siempre" se presentaron casos de delitos informáticos.

Estos resultados evidencian que los delitos informáticos son un problema significativo en la región, lo que coincide con estudios previos a nivel

nacional e internacional. En el ámbito internacional, Zamora (2011) señala que la criminalidad informática ha evolucionado y se ha convertido en una amenaza global debido a la dificultad para rastrear a los delincuentes y la falta de regulaciones uniformes. En Guatemala, por ejemplo, la legislación desactualizada ha propiciado un incremento de estos delitos, una problemática que podría replicarse en Coronel Portillo, donde la población percibe una alta frecuencia de delitos informáticos.

Por otro lado, Tornel (2022) enfatiza que, a pesar de los esfuerzos de la Unión Europea por establecer normativas de ciberseguridad, la falta de armonización legislativa y la complejidad en la obtención de pruebas digitales han limitado la persecución de estos delitos. En este sentido, los resultados de Coronel Portillo podrían estar influenciados por dificultades similares en la regulación y aplicación de leyes que combatan eficazmente los delitos informáticos.

A nivel nacional, Carbajal (2022) identifica que el fraude informático es el delito con mayor incidencia en el Perú dentro de los delitos informáticos, incluyendo la clonación de tarjetas, el phishing y las transferencias fraudulentas. Sin embargo, la Ley Nº 30096 no tipifica adecuadamente muchas de estas modalidades, lo que dificulta la persecución penal. Esta falta de actualización normativa podría explicar la percepción de alta incidencia de delitos informáticos en Coronel Portillo, donde los ciudadanos pueden sentirse desprotegidos ante estas amenazas.

Desde una perspectiva local, Cataño y Panduro (2023) encontraron que los delitos informáticos afectan significativamente las operaciones financieras de los bancos en la provincia de Coronel Portillo. La correlación entre delitos digitales y fraudes bancarios sugiere que la alta frecuencia de delitos informáticos reportada en esta investigación podría estar vinculada a la vulnerabilidad del sector financiero ante estas amenazas.

Asimismo, Díaz y Huamán (2022) identificaron una relación entre el lavado de dinero y el uso de criptomonedas para actividades delictivas en la provincia de Coronel Portillo. Esto indica que los delitos informáticos no solo afectan a individuos y empresas, sino que también pueden estar relacionados con estructuras criminales más amplias, lo que explicaría la alta percepción de su ocurrencia en la región.

En conclusión, los resultados de esta investigación muestran que la Variable Delitos Informáticos es una problemática relevante en la provincia de Coronel Portillo, con un 30.00% de los encuestados afirmando que estos delitos "casi siempre" ocurren y un 31.25% indicando que "siempre" están presentes. Estos hallazgos coinciden con estudios previos que han señalado la falta de regulación actualizada, la insuficiencia de recursos tecnológicos y la creciente sofisticación de los ciberdelincuentes como factores que favorecen la proliferación de estos delitos. Para abordar esta problemática, es fundamental fortalecer el marco legal, mejorar la ciberseguridad en el sector financiero y promover campañas de concienciación sobre la prevención de delitos informáticos en la población.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- En relación con el objetivo general, que fue determinar la relación existente entre la ciberdelincuencia y los delitos informáticos en la provincia de Coronel Portillo durante el 2023, se concluye que ambas variables mantienen una asociación significativa y positiva, lo que se evidencia en un coeficiente de correlación Rho de Spearman de 0.855 ($p = 0.000$). Este resultado confirma que el incremento de la ciberdelincuencia incide directamente en la ocurrencia de delitos informáticos en el contexto local.

- Respecto al primer objetivo específico, orientado a determinar cómo se relaciona el marco legal con los delitos informáticos, los resultados evidenciaron un coeficiente de correlación de 0.864 ($p = 0.000$), lo que demuestra que la eficacia, actualización y aplicación de las normas jurídicas son factores decisivos para prevenir, regular y sancionar las conductas vinculadas a la ciberdelincuencia.

- En cuanto al segundo objetivo específico, que buscó analizar la relación entre las tipologías de ciberdelincuencia y los delitos informáticos, se verificó que estas (hurto, fraude, estafa y sabotaje

informático) presentan una correlación altamente significativa (Rho = 0.877; p = 0.000). Este hallazgo confirma que la diversidad de modalidades delictivas digitales incrementa la frecuencia y complejidad de los delitos informáticos en la provincia.

- Con relación al tercer objetivo específico, que consistió en determinar la relación entre la seguridad pública y los delitos informáticos, se estableció un coeficiente de correlación de 0.847 (p = 0.000), lo cual refleja que el nivel de control institucional y de protección ciudadana incide de manera directa en la reducción o proliferación de estas conductas ilícitas.

- Finalmente, en lo que respecta al cuarto objetivo específico, referido al incremento de la ciberdelincuencia y su vínculo con los delitos informáticos, se obtuvo un coeficiente de correlación de 0.884 (p = 0.000), evidenciando que el crecimiento sostenido de actividades delictivas en el entorno digital se encuentra directamente asociado con el aumento de la incidencia de delitos informáticos en la provincia de Coronel Portillo.

5.2. Recomendaciones

- Se recomienda la implementación de estrategias de ciberseguridad más efectivas en el sector privado y público, con un enfoque en la actualización de marcos normativos y sanciones más severas para delitos informáticos. Además, es fundamental incentivar la investigación académica sobre nuevas amenazas cibernéticas y su impacto en las empresas para desarrollar medidas de protección más eficaces.

- Se sugiere diseñar campañas educativas dirigidas a la población de Coronel Portillo sobre los riesgos de la ciberdelincuencia y las mejores prácticas de seguridad digital. Las universidades y centros de investigación pueden colaborar con entidades gubernamentales para difundir información preventiva y desarrollar guías prácticas de protección contra delitos informáticos.

- Se recomienda incluir en los planes educativos programas de alfabetización digital, con especial énfasis en comunidades vulnerables. Además, las instituciones académicas y gubernamentales deben desarrollar estudios sobre el impacto de la desigualdad económica en la proliferación de delitos informáticos, para diseñar políticas públicas más inclusivas y efectivas en la reducción de estos crímenes.

- Se recomienda fortalecer la formación en ciberseguridad de las fuerzas del orden mediante capacitaciones especializadas y la incorporación de nuevas tecnologías en la investigación de delitos informáticos. Además, se sugiere la creación de unidades especializadas en delitos cibernéticos dentro de las entidades de seguridad pública para una respuesta más eficiente.

- Se sugiere que las instituciones académicas realicen estudios continuos sobre el impacto del crecimiento digital en la seguridad cibernética de Coronel Portillo. Asimismo, es importante fomentar el desarrollo de infraestructura tecnológica segura y la aplicación de normativas de ciberseguridad obligatorias para empresas y usuarios con el fin de minimizar la exposición a amenazas digitales.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez Pozo, M. (2007). *Concurso ideal de delitos.* España.

Baena Paz, G. (2017). *Metodología de la investigación: Serie integral por competencias.* México: Grupo Editorial Patria.

Bank, A. (2020). *Ciberseguridad riesgos y avances y el camino a seguir América Latina y el Caribe.* Caribe.

Barrera Baron, J. A. (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede seccional Sogamoso 2016.*

Canedo Estrad, A. (2010). *La informática forense y los delitos informáticos.* Revista Pensamiento Americano. ISSN: 2027-2448 No.4.

Carbajal Camones, M. (2022). *Las fiscalías especializadas en delitos informáticos.* Lima.

Cárdenas Aravena, C. (2008). *El lugar de comisión de los denominados ciberdelitos.*

Cataño Bardales, T. & Panduro Arévalo, L. (2023). *El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo - Ucayali, 2022.* Pucallpa.

Custodio Cumpa, Y. (2021). *Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático.* Chiclayo.

Chiriboga Guzmán, A. (2021). *La Ciberdelincuencia y el delito contra la libertad sexual, Comas, 2021.* Lima.

Díaz Martinez, D. & Huamán Ayala, M. (2022). *Lavado de dinero y crimen organizado a través de las cripto monedas en la provincia de Coronel Portillo, 2021.* Pucallpa.

Espinoza Malca, J. (2022). *Factores que inciden en la tipicidad objetiva del delito de fraude informático, Ministerio Público Chepén, 2022 .* Chepén.

Gómez Rodríguez, Á. (2021). *Aspectos procesales de los delitos informáticos y tecnológicos.* España.

Gómez, J. (2019). *El tratamiento jurídico penal por parte del fiscal en los delitos informáticos contra el patrimonio, distrito judicial de Lima Norte 2019.* Lima.

Hidalgo, C. N., & Solano, G. S. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento Jurídico Peruano. Propuesta de incorporación del artículo 7-a en la ley de delitos informáticos 30096".*

Huamán Cruz, M. (2020). *Los delitos informaticos en Perú y la suscripción del convenio de budapest.* Cuzco.

Lamperti, S. (2017). *Los Delitos Informáticos. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense.*

Leyva Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Revista Lucerna Iuris Et Investigatio*, 29-47.

López, M. (2021). *Qué es el vishing: estafa a través de llamadas o mensajes de voz.* Lima.

Marín Ampuero, A., & Santa Maria Flores, E. (2021). *El ciberdelito de redes delictivas a escala.* Pucallpa.

Mata, R. (2007). *Delitos cometidos mediante sistemas informáticos.* Bilbao.

Mayer, L., & Oliver, G. (2020). *El delito de fraude informático: concepto y delimitación.* Chile.

Mengoa Valdivia, M. (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.* LIMA.

Morales Delgado, D. (2016). *La inseguridad al utilizar los servicios de redes.* Pimentel.

Ochoa Marcillo, A. (2021). *Desafíos globales del cibercrimen Caso Ecuador periodo 2014-2019.* Quito.

Ortiz Ruiz, A. (2012). *El uso de recursos tecnológicos para el desarrollo de competencias cognitivas y de acción en alumnos de tercer grado de preescolar.* México.

Oxman, N. (2013). Estafas informáticas a través de internet: acerca de la imputación penal del "phishing" y el "pharming". *Revista de derecho (Valparaíso)*, (41), 211-262.

Pérez Luño, A. (2000). *La tutela de la libertad informática en la sociedad globalizada.* Sevilla.

Proaño, R., & Gavilanes, A. (2019). *Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana.* Ecuador.

Quiroga Mendoza, O. (2018). *El tratamiento jurídico y legal de la libertad e indemnidad sexual en el código penal peruano.* Chiclayo.

Quiroz Tirado, A. (2018). *La imputación del delito de falsedad genérica en las fiscalías provinciales penales corporativas de Cajamarca desde el 01 de abril de 2010 al 31 de agosto de 2015.* Cajamarca.

Rayón Ballesteros, M., & Gómez Hernández, J. (2014). *Cibercrimen: particularidades en su investigación y enjuiciamiento.* Madrid.

Rincón Ríos, J. (2015). *El delito en la cibersociedad y la justicia penal internacional.* Madrid.

Rodríguez García, J. D. (2020). *Una aproximación al delito de estafa en sus modalidades clásica e informática: De la estafa tradicional a las nuevas modalidades como el Phishing.* Lima.

Rodriguez Zevallos, C. (2018). *Metodología de clasificación de delitos informáticos.* Quito.

Temperini, I. (2013). *Delitos informáticos en Latinoamérica: Un estudio de derecho comparado.*

Tornel Estrada, M. (2022). *La ciberdelincuencia y las especialidades procesales de la prueba.* Madrid.

Ventura Quijano, A. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020.* Lima.

Villavicencio Terreros, F. (2014). *Delitos informáticos.* LIMA.

Zamora Alvizures, J. (2011). *Implementación de la informática forense en la obtención de evidencia digital para combatir los delitos informáticos Guatemala.*

ANEXOS

ANEXO 1

MATRIZ DE CONSISTENCIA

<table>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES</th><th>METODOLOGÍA</th></tr>
<tr>
<td>Problema General
¿Cómo se relaciona la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023?</td>
<td>Objetivo General
Determinar qué relación existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.</td>
<td>Hipótesis General
Existe relación significativa existe entre la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023</td>
<td rowspan="2">Variable Independiente
Ciberdelincuencia

Dimensiones:
• Delitos computacionales
• Tasa de incidencia de delitos informáticos.
• Índice de seguridad cibernética.

Variable Dependiente
Delitos informáticos

Dimensiones:
• Hurto informático
• Fraude informático
• Estafa informática
• Sabotaje informático</td>
<td rowspan="2">Tipo de Investigación:
Básica.

Diseño
Descriptivo- Correlacional

Población
Estará compuesta por 30 carpetas fiscales en la Primera Fiscalía Penal Corporativa de la provincia de Coronel Portillo, Diez (10) Fiscales de la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo y 2580 Abogados litigantes.

Muestra
Estará compuesta por 20 Carpetas fiscales de ciberdelincuencia en la Primera Fiscalía Penal Corporativa de Coronel Portillo, Diez (10) Fiscales de la Primera Fiscalía Penal Corporativa de la Provincia de Coronel Portillo y 50 Abogados litigantes.

Técnicas
Ficha de análisis documental
Encuesta

Instrumento
Cuestionario.</td>
</tr>
<tr>
<td>Problemas Específicas

¿Cómo se relaciona el panorama actual de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023?

¿Cómo se relacionan los factores socioeconómicos, tecnológicos y culturales con la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023?

¿Cómo se relaciona en la seguridad pública en relación a la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023?

¿Cómo se relaciona el aumento de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023?</td>
<td>Objetivos Específicos

Analizar qué relación existe entre el panorama actual de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Evaluar qué relación existe entre los factores socioeconómicos, tecnológicos y culturales con la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Determinar qué relación existe entre en la seguridad pública en relación a la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Analizar qué relación existe entre el aumento de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.</td>
<td>Hipótesis Específicas

Existe relación entre el panorama actual de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023

Existe relación entre los factores socioeconómicos, tecnológicos y culturales con la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Existe relación entre en la seguridad pública en relación a la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.

Existe relación entre el aumento de la ciberdelincuencia y delitos informáticos en la provincia de Coronel Portillo 2023.</td>
</tr>
</table>

ANEXO 2

INSTRUMENTO DE APLICACIÓN

VARIABLE 1: CIBERDELINCUENCIA

Dimensión 1: Delitos Computacionales

1. En mi opinión, los delitos computacionales son una preocupación importante en la sociedad actual.

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

2. Creo que la piratería informática es un problema significativo en el ámbito digital.

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

3. Considero que el fraude en línea es una forma común de delito computacional.

   A) Nunca

   B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

4. Los ataques de malware son una amenaza frecuente en el entorno digital.

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

5. La suplantación de identidad en línea es un problema grave en términos de delitos computacionales.

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

6. Considero que el robo de información personal en línea es un delito cada vez más común.

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

7. En mi experiencia, el phishing es una táctica utilizada con frecuencia por los delincuentes informáticos.

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

8. Creo que el sabotaje de sistemas informáticos es una amenaza seria en el mundo digital.

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

Dimensión 2: Tasa de Incidencia de Delitos Informáticos

9. He sido víctima de algún tipo de delito informático en el pasado.

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

10. En general, ¿crees que la incidencia de delitos informáticos está aumentando en la sociedad?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

11. ¿Con qué frecuencia escuchas o lees noticias sobre delitos informáticos en los medios de comunicación?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

12. ¿Conoces a alguien cercano que haya sido víctima de un delito informático?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

13. ¿Consideras que la mayoría de los delitos informáticos quedan impunes?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

14. En tu opinión, ¿las autoridades son efectivas en la persecución de los delitos informáticos?

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

15. ¿Crees que las personas toman suficientes medidas de seguridad para protegerse contra los delitos informáticos?

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

16. ¿Te sientes seguro/a al realizar transacciones financieras en línea debido a la amenaza de delitos informáticos?

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

Dimensión 3: Índice de Seguridad Cibernética

17. En mi opinión, la seguridad cibernética es una preocupación crucial para las empresas y organizaciones.

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

18. Creo que las empresas deberían invertir más en medidas de seguridad cibernética.

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

19. En mi lugar de trabajo, se toman medidas efectivas para proteger los datos contra amenazas cibernéticas.

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

20. Considero que la educación sobre seguridad cibernética debería ser más prioritaria en las instituciones educativas.

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

21. En mi hogar, se implementan medidas de seguridad cibernética para proteger los dispositivos y la información.

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

22. Creo que las leyes y regulaciones relacionadas con la seguridad cibernética son adecuadas y efectivas.

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

23. En general, ¿te sientes seguro/a en línea debido a las medidas de seguridad cibernética que existen?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

24. Considero que la conciencia pública sobre la importancia de la seguridad cibernética es suficiente.

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

VARIABLE 2: DELITOS INFORMÁTICOS

Dimensión 1: Hurto Informático

1. ¿Con qué frecuencia ha experimentado el robo de información personal a través de medios electrónicos?

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

2. ¿En qué medida cree que su información financiera ha sido vulnerada en línea sin su consentimiento?

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

3. ¿Con qué frecuencia ha sido víctima de la apropiación no autorizada de sus datos en línea?

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

4. ¿Cuántas veces ha sido testigo de la sustracción de propiedad intelectual en línea?

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

5. ¿Con qué frecuencia ha detectado intrusiones en sus cuentas en línea sin su autorización?

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

6. ¿En qué medida ha sufrido la pérdida de datos personales debido a un ataque informático?

   A) Nunca

   B) Casi Nunca

   C) A veces

   D) Casi Siempre

   E) Siempre

7. ¿Con qué frecuencia ha sido afectado por el secuestro de información o archivos en su computadora?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

Dimensión 2: Fraude Informático

8. ¿Con qué frecuencia ha sido víctima de suplantación de identidad en línea?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

9. ¿En qué medida ha sido engañado por correos electrónicos fraudulentos solicitando información personal?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

10. ¿Cuántas veces ha experimentado la manipulación de transacciones financieras en línea sin su consentimiento?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

11. ¿Con qué frecuencia ha sido víctima de estafas en línea que prometen beneficios falsos?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

12. ¿En qué medida ha sido afectado por la publicidad engañosa en línea que lo dirige a sitios fraudulentos?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

13. ¿Cuántas veces ha sido objeto de fraudes en línea relacionados con la compra de productos o servicios?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

14. ¿Con qué frecuencia ha sido engañado por programas maliciosos que comprometen la seguridad de su información en línea?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

Dimensión 3: Estafa Informática

15. ¿Con qué frecuencia ha sido objeto de falsificación de documentos electrónicos?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

16. ¿En qué medida ha sido afectado por esquemas de phishing diseñados para robar información personal?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

17. ¿Cuántas veces ha sido engañado por páginas web falsas que imitan a sitios legítimos para recopilar datos personales?

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

18. ¿Con qué frecuencia ha sido víctima de estafas en línea que involucran la venta de productos o servicios falsos?

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

19. ¿En qué medida ha sido afectado por esquemas de inversión fraudulentos en línea?

    A) Nunca

    B) Casi Nunca

    C) A veces

    D) Casi Siempre

    E) Siempre

20. ¿Cuántas veces ha sido engañado por ofertas falsas de empleo en línea diseñadas para obtener su información personal?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

21. ¿Con qué frecuencia ha sido objeto de estafas en línea relacionadas con premios o sorteos falsos?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

Dimensión 4: Sabotaje Informático

22. En los últimos 6 meses, ¿con qué frecuencia ha experimentado intentos de intrusión no autorizados en su sistema informático?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

23. ¿Con qué frecuencia ha notado cambios no autorizados en los archivos o programas de su sistema informático?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

24. ¿Con qué frecuencia ha encontrado evidencia de software malicioso (como virus, troyanos, etc.) en su sistema informático?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

25. ¿Con qué frecuencia ha experimentado fallos significativos en su sistema informático que parecían ser el resultado de acciones maliciosas?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

26. ¿Con qué frecuencia ha recibido amenazas o demandas de rescate relacionadas con el funcionamiento de su sistema informático?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

27. ¿Con qué frecuencia ha tenido problemas de seguridad como resultado de empleados descontentos o ex empleados que han accedido a su sistema informático de manera no autorizada?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre

28. ¿Con qué frecuencia ha sido objeto de ataques de denegación de servicio que han afectado la disponibilidad de su sistema informático?

A) Nunca

B) Casi Nunca

C) A veces

D) Casi Siempre

E) Siempre