Universidad Nacional
SAN LUIS GONZAGA

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"

FACULTAD DE DERECHO Y CIENCIA POLITICA

"AÑO DE LA ESPERANZA Y EL FORTALECIMIENTO DE LA DEMOCRACIA"

....

EVALUACION DE ORIGINALIDAD

CONSTANCIA

El que suscribe, deja constancia que se ha realizado el análisis con el software de verificación de similitud de **TESIS, cuyo** título es:

LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024

Presentado por:

BONIFAZ MUÑOZ, MARIO FRANCISCO

Que, conforme al informe automatizado de originalidad emitido por el Operador del Programa Informático Evaluador de Originalidad de la Facultad de Derecho y Ciencia Política de la UNICA, se concluye que;

El resultado obtenido es del 4% por el cual se le otorga el calificativo APROBADO, según Reglamento de Evaluación de la Originalidad

Para dar fe, se adjunta al presente el reporte de similitud de las bases de datos de Ithenticate.

Ica, 17 de Marzo del 2026

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"
FACULTAD DE DERECHO Y CIENCIA POLITICA
DIRECCIÓN DE UNIDAD DE INVESTIGACIÓN

Dra. ROSALINA TRAVEZAN MOREYRA
DIRECTORA

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA”

VICERECTORADO DE INVESTIGACIÓN

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

“Los delitos informáticos y su regulación en el sistema penal: un análisis de los nuevos desafíos en la era digital del distrito fiscal de Ica, año 2024”

LÍNEA DE INVESTIGACIÓN

SOCIEDAD, DESARROLLO SOSTENIBLE, POLÍTICAS PÚBLICAS Y AMBIENTALES

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

Presentado por:

Bach. BONIFAZ MUÑOZ, MARIO FRANCISCO

ASESOR: Dr. JULIO CESAR GIRAO OLAECHEA

ICA – PERÚ

2025

DEDICATORIA

A mi familia, por ser el pilar fundamental que sostuvo cada uno de mis pasos a lo largo de este camino académico. A mis padres, por su entrega incondicional, por enseñarme con su ejemplo el valor del esfuerzo, la responsabilidad y la perseverancia; y por creer en mí incluso en los momentos de mayor dificultad. A mis hermanos, por su apoyo constante, su comprensión y sus palabras de aliento, que fueron un impulso permanente para no rendirme. A todos ellos, mi gratitud eterna, pues sin su amor, paciencia y respaldo, la culminación de este logro no habría sido posible.

Mario Francisco.

AGRADECIMIENTOS

A las autoridades de la Alta Dirección de la Universidad Nacional “San Luis Gonzaga” de Ica, por su conducción responsable y su firme compromiso con el fortalecimiento institucional, los cuales han permitido consolidar una universidad con licenciamiento vigente, orientada a la calidad académica y al servicio de la sociedad.

Al Dr. Wenceslao Miguel Quispe Segovia, decano de la Facultad de Derecho y Ciencia Política, autoridades y al personal administrativo de la Facultad de Derecho de la Universidad Nacional “San Luis Gonzaga” de Ica, por el respaldo constante, la disposición permanente y el esfuerzo sostenido en favor de nuestra formación profesional y académica.

A los docentes de la Facultad, por su esfuerzo, compromiso y valiosa entrega en la transmisión del conocimiento, contribuyendo a nuestro desarrollo académico y personal.

Al Dr. Julio Cesar Girao Olaechea, por su asesoría, acompañamiento continuo y valiosos aportes durante el desarrollo de la presente investigación, desempeñando con compromiso y responsabilidad su labor como Asesor de Tesis.

A mis compañeras y compañeros de aula y de trabajo, por la solidaridad, el apoyo mutuo, la amistad y el intercambio de experiencias, que enriquecieron nuestro proceso de aprendizaje y fortalecieron nuestro crecimiento colectivo.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La tesis titulada “LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024” tuvo como propósito principal analizar de qué manera los delitos informáticos suponen un desafío para la regulación penal en el Distrito Fiscal de Ica, año 2024

Para su elaboración, se tuvo en consideración el siguiente conjuntos de normas: la Constitución Política del Perú de 1993; la Ley N.º 30220, Ley Universitaria; el Estatuto de la Universidad Nacional San Luis Gonzaga (UNICA); la Resolución Rectoral N.º 029-2021-R, que establece las Líneas de Investigación de la UNICA; la Resolución Rectoral N.º 048-2021-R, correspondiente al Reglamento de Grados y Títulos; y la Resolución Rectoral N.º 1320-2021-R, que aprueba la Guía para la Elaboración de Proyecto de Tesis y Tesis. Asimismo, el Código Penal, Código Procesal Penal, Ley Nº 30096 - Ley de Delitos Informáticos; Ley 32314: modifican el Código Penal y otro para sancionar el uso de la inteligencia artificial en la comisión de delitos; entre otros.

Para recolección de datos se aplicó la técnica de la encuesta, utilizando como instrumentos los cuestionarios sobre los delitos informáticos y la regulación penal en la era digital.

Se llegó a la conclusión de que los delitos informáticos constituyen un verdadero desafío con relación a la eficacia de la regulación penal en la era digital

PALABRAS CLAVE: ciberdelincuencia, era digital, phishing, fraude informático.

ABSTRACT

The thesis entitled "COMPUTER CRIMES AND THEIR REGULATION IN THE CRIMINAL JUSTICE SYSTEM: AN ANALYSIS OF THE NEW CHALLENGES IN THE DIGITAL AGE OF THE ICA DISTRICT ATTORNEY'S OFFICE, YEAR 2024" had as its main purpose to analyze how computer crimes pose a challenge to criminal regulation in the Ica District Attorney's Office in the year 2024.

The following set of regulations was taken into consideration in its preparation: the 1993 Political Constitution of Peru; Law No. 30220, University Law; the Statute of the National University of San Luis Gonzaga (UNICA); Rector's Resolution No. 029-2021-R, which establishes the UNICA's Lines of Research; Rector's Resolution No. 048-2021-R, corresponding to the Regulations on Degrees and Titles; and Rector's Resolution No. 1320-2021-R, which approves the Guide for the Preparation of Thesis Projects and Theses. Likewise, the Criminal Code, Criminal Procedure Code, Law No. 30096 - Law on Computer Crimes; Law 32314: amend the Criminal Code and another to punish the use of artificial intelligence in the commission of crimes; among others.

For data collection, the survey technique was applied, using questionnaires on computer crimes and criminal regulation in the digital age as instruments.

It was concluded that computer crimes constitute a real challenge in relation to the effectiveness of criminal regulation in the digital age.

KEY WORDS: cybercrime, digital age, phishing, computer fraud.

I. INTRODUCCIÓN

Los delitos informáticos son reconocidos cada vez más como una de las principales amenazas en la era digital a nivel internacional, con repercusiones directas en la seguridad jurídica, económica y social de los Estados. La rápida expansión del uso de tecnologías de la información y de plataformas digitales ha facilitado la proliferación de conductas ilícitas como el phishing, el fraude electrónico, la suplantación de identidad y el acceso no autorizado a sistemas informáticos. Estas prácticas delictivas generan graves afectaciones a los derechos fundamentales de las personas, tales como el patrimonio, la intimidad y la seguridad de la información. Asimismo, la dificultad para identificar a los responsables y la naturaleza transnacional de estos delitos complican la labor de los sistemas penales, generando altos niveles de impunidad y debilitando la confianza ciudadana en las instituciones encargadas de administrar justicia.

En diversos países de América Latina se han adoptado reformas normativas orientadas a enfrentar el cibercrimen. Un ejemplo de ello es Ecuador, cuyo Código Orgánico Integral Penal, vigente desde el año 2014, tipifica delitos como el acceso ilícito a sistemas informáticos, el sabotaje informático y el phishing. No obstante, pese a estos avances legislativos, la constante evolución tecnológica continúa superando la capacidad de respuesta de los Estados, evidenciando limitaciones en la aplicación de la norma penal, dificultades en la investigación digital y vacíos legales frente a nuevas modalidades delictivas. Esta realidad ha generado consecuencias negativas, tales como el incremento de denuncias, la saturación de los órganos de justicia y la persistencia de una respuesta penal insuficiente frente a los delitos informáticos.

En el Perú, esta problemática ha sido abordada mediante la promulgación de la Ley N.° 30096, Ley de Delitos Informáticos, que tiene por finalidad proteger los sistemas informáticos, la información digital y los derechos de los ciudadanos frente a conductas ilícitas cometidas en el entorno virtual. No obstante, pese a su importancia, la aplicación de esta normativa presenta serias limitaciones, entre las que destacan la falta de actualización frente a nuevas formas de criminalidad digital, la ambigüedad en la tipificación de determinadas conductas y la insuficiente especialización de los operadores del sistema de justicia. Asimismo, la carencia de herramientas tecnológicas adecuadas dificulta la investigación, persecución y sanción efectiva de estos delitos, afectando la eficacia del sistema penal en su conjunto.

En la región Ica, esta problemática no resulta ajena, por cuanto el incremento de los delitos informáticos se ha convertido en un factor que limita la eficacia de la regulación penal y la capacidad de respuesta del sistema de justicia. Es de verse que, en los últimos años, se ha registrado un aumento de denuncias relacionadas con estafas digitales, fraudes electrónicos, uso indebido de plataformas virtuales y difusión no autorizada de información personal. Sin embargo, esta creciente incidencia delictiva no ha sido atendida de manera adecuada, debido a la escasa presencia de fiscales especializados en criminalidad informática, la limitada capacitación en técnicas de investigación digital y la falta de recursos tecnológicos. Esta situación genera retrasos en los procesos, dificulta la identificación de los responsables y contribuye a una percepción de impunidad que afecta directamente a las víctimas.

Bajo este panorama, la presente investigación tiene por finalidad describir, analizar y explicar de manera detallada cómo los delitos informáticos representan un desafío creciente para la regulación penal en la era digital en el Distrito Fiscal de Ica. Para ello, no solo se evalúan las limitaciones normativas existentes, sino también las dificultades operativas del sistema penal, tales como la insuficiencia de herramientas tecnológicas, la falta de especialización del personal y los vacíos legales frente a nuevas modalidades delictivas. Los delitos informáticos, entendidos como conductas ilícitas que se cometen mediante el uso de tecnologías digitales, adquieren una relevancia particular en un contexto de creciente digitalización de las actividades económicas, sociales y administrativas, donde la vulnerabilidad de los ciudadanos frente al cibercrimen se incrementa de manera significativa.

La importancia del estudio radica en que aporta evidencia objetiva y sistemática sobre una problemática que, si bien ha sido reconocida por las autoridades y por la ciudadanía, aún no ha sido abordada con la profundidad analítica necesaria en el ámbito académico regional. El Distrito Fiscal de Ica, al igual que otras regiones del país, enfrenta el reto de adaptar su sistema penal a las exigencias de la era digital, en un contexto marcado por limitaciones presupuestales, carencias tecnológicas y una creciente demanda de justicia por parte de las víctimas de delitos informáticos. Esta situación no solo afecta la eficacia del sistema penal, sino que compromete la protección de los derechos fundamentales y la seguridad jurídica de la población.

Asimismo, la presente investigación se sustenta en antecedentes nacionales e internacionales que evidencian la relación directa entre el avance del cibercrimen y la necesidad de contar con una regulación penal moderna, dinámica y especializada. Diversos estudios han demostrado que la ausencia de una respuesta penal eficaz frente a los delitos informáticos incrementa la reincidencia delictiva, debilita el efecto disuasivo de la norma penal

y genera desconfianza en las instituciones de justicia, especialmente en contextos regionales donde la capacidad operativa es limitada.

Finalmente, se plantea que los resultados obtenidos permitirán dimensionar con mayor claridad la magnitud del problema en el Distrito Fiscal de Ica, así como formular recomendaciones orientadas a fortalecer la regulación penal, mejorar la capacitación de los operadores de justicia y promover el uso de herramientas tecnológicas adecuadas para la investigación del cibercrimen. En tal sentido, la investigación denominada "LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024" tiene por finalidad dotar de información suficiente y veraz sobre el problema objeto de estudio, contribuyendo al fortalecimiento del sistema penal y a la protección efectiva de los derechos de los ciudadanos en el entorno digital.

En lo que corresponde a los **Antecedentes Internacionales** tenemos a:

Colorado (2025) quien en su investigación tuvo como propósito "examinar de qué manera los delitos cibernéticos afectan los derechos fundamentales, poniendo especial atención al marco normativo ecuatoriano y su relación con los estándares internacionales, cuya metodología empleada fue de enfoque integral y método descriptivo; permitiendo llegar así a la conclusión:

"La digitalización ha revolucionado el manejo de datos personales, generando amenazas vinculadas a delitos cibernéticos. Aunque Ecuador fortaleció su legislación con la Ley Orgánica de Protección de Datos Personales en 2021, alineada a los estándares internacionales como el Reglamento General de Protección de Datos, empero, aún enfrenta retos en su aplicación y adecuación institucional ante innovaciones tecnológicas". (p. 2363) Las investigaciones internacionales evidencian que la ausencia de estrategias eficaces en la ciberseguridad puede provocar filtraciones significativas de información personal, comprometiendo la privacidad de millones, tales situaciones resaltan la urgencia de fortalecer las normas legales y fomentar una conciencia sobre la protección de datos.

Macias et.al. (2022) quienes en su estudio que realizado tuvieron por objetivo "dar a conocer las técnicas que utilizan los ciberdelincuentes en el Ecuador, socializar la penalización y sugerencias para evitar ser víctima de este tipo de delitos; donde se empleó la metodología Estudio de Mapeo Sistemático; teniendo como resultado que: Dado que los delitos informáticos perjudican a personas y a entidades públicas y privadas que utilizan tecnología e internet, es fundamental establecer políticas y protocolos de seguridad, además de capacitar continuamente

al personal en medidas informáticas para reducir riesgos". (p. 242) Es fundamental que los usuarios de internet estén informados sobre las sanciones que establece el Código Integral Penal del Ecuador respecto a los delitos informáticos, para reconocer si han sido afectados o están infringiendo la ley; además, el Estado debe fomentar capacitaciones y difusión sobre el uso responsable de la tecnología y la prevención de estos delitos.

Diaz et. al. (2023) en su investigación tuvo como objetivo "analizar la interpretación subjetiva de las leyes y la brecha de conocimiento en torno a los delitos cibernéticos, cuya metodología empleada fue de enfoque mixto cuali-cuantitativa, el análisis documental llega a la conclusión que, la perspectiva legal de los delitos informáticos es vital para proteger la privacidad y los datos personales, así como garantizar la estabilidad económica de personas y empresas, una regulación efectiva ayuda a prevenir fraudes electrónicos y amenazas a la seguridad financiera". (p.753) El marco legal ecuatoriano requiere incorporar nuevas tipificaciones penales que sancionen más conductas, tanto por acción como por omisión, realizadas a través de mecanismos informáticos, electrónicos y redes digitales, buscando cubrir diversas amenazas contra el Estado o la sociedad y reforzar así la seguridad jurídica.

Jara; Durán (2025) llevaron a cabo una investigación cuya finalidad principal fue analizar la situación de la ciberdelincuencia en Ecuador, evaluando los desafíos legales y la efectividad de las políticas públicas. El estudio se llevó a cabo utilizando una metodología cualitativa, basada en la revisión de literatura, informes oficiales y entrevistas con expertos en ciberseguridad. Los autores llegaron a la conclusión de que, a pesar de los esfuerzos por mejorar la ciberseguridad, las políticas existentes no lograron frenar el aumento de los ciberdelitos, la legislación no se actualizó de manera adecuada para enfrentar las nuevas amenazas digitales, y la cooperación internacional siguió siendo limitada (p. 2). Al respecto resulta preciso señalar que el Derecho debe de ser dinámico y adecuarse a los diferentes avances tecnológicos, de modo que para enfrentar los delitos informáticos se cuente sistema normativo idóneo y eficaz.

Corrales (2024) realizó una investigación cuyo objetivo principal fue "analizar la evolución y el impacto del ciberdelito en la era digital y cómo afecta el derecho a la privacidad en el ciberespacio; siendo desarrollada bajo una metodología cualitativa, que revela la complejidad del ciberdelito en la era actual y subraya la importancia crítica de abordar estas cuestiones desde múltiples perspectivas, integrando consideraciones legales, técnicas, éticas y políticas" (p.5). La conclusión a la que arribó el autor es que, En la era digital, los ciberdelitos presentan una serie de desafíos complejos que requieren un análisis profundo desde el derecho penal, tanto en su estructura básica como en su aplicación pura (p.37). Al respecto cabe mencionar que, para combatir la criminalidad informática o ciberdelincuencia, no basta con

producir leyes que en apariencia resulten eficaces; sino que es necesario realizar un estudio criminológico sobre esta novedosa forma de cometer delitos, para de ese modo adoptar políticas criminales adecuadas y de utilidad pragmática; que ayuden a enfrentar con eficacia la ciberdelincuencia.

En cuanto a los **Antecedentes Nacionales** se consideraron a:

Muñoz (2024) quien en su estudio que realizo tuvo por objetivo "determinar la influencia de la cultura judicial del derecho penal para la regulación de los delitos informáticos en el Distrito judicial de Pasco, 2021, donde se empleó una investigación de tipo descriptivo y correlacional; permitiendo llegar así a la conclusión que, la cultura judicial en el ámbito penal favorece la regulación de los delitos informáticos, ya que el análisis de sentencias reflejó una administración justa, imparcial y conforme al debido proceso, respetando la legalidad y garantizando la seguridad jurídica en Pasco, 2021". (p.70) El rigor excesivo en los conocimientos del derecho penal y procesal penal debe dejarse atrás frente a la falta de información, desinterés y desconocimiento por parte de magistrados, fiscales, funcionarios, abogados y ciudadanos, promoviendo así el acceso a la cultura judicial penal y la adecuada regulación de los delitos informáticos.

Rojas (2024) quien en su estudio que realizo tuvo por objetivo "analizar la necesidad de regular nuevas modalidades del delito de fraude informático frente a la ciberdelincuencia en el Perú 2023, con una metodología cualitativa con un enfoque no experimental; teniendo como resultado que: Ante el avance de aplicaciones, plataformas, sistemas operativos y servidores, resulta indispensable implementar una normativa que contemple las nuevas modalidades de fraude informático en Perú, permitiendo sancionar con precisión las técnicas utilizadas por los ciberdelincuentes". (p. 98) La falta de legislación específica facilita la evasión de responsabilidades penales, por lo que se requiere una regulación más rigurosa basada en la imputación objetiva, esta medida no solo contribuirá a castigar adecuadamente estas conductas, sino también a proteger mejor a las víctimas y garantizar una respuesta eficiente del sistema de justicia frente a la ciberdelincuencia.

Rosales (2024) quienes en su estudio que realizaron tuvieron por objetivo "determinar de qué manera se relaciona el incremento de los delitos informáticos y su problemática con la impunidad delictiva en Lima, 2024, donde se empleó una metodología de enfoque cuantitativo, no experimental y de tipo correlacional de corte transversal; lo que lleva a la conclusión: La criminalidad informática está vinculada a la carencia de sanciones eficaces en Lima, ya que los ciberdelincuentes actúan con mayor libertad al no enfrentar consecuencias penales, lo que

fomenta la impunidad en el ámbito informático". (p.33) Se debe promover estudios especializados en comisiones legislativas que analicen y actualicen continuamente el aumento de delitos informáticos, buscando unificar criterios para reducir la impunidad generada por el anonimato del ciberdelincuente, para ello, se tiene que examinar el desarrollo del Derecho Procesal Penal y la sanción efectiva.

Vinelli (2021) realizó una investigación cuyo objetivo principal fue Analizar la vinculación entre los delitos informáticos y la criminalidad económica (p.95). Se trato de una investigación de tipo básica, con un diseño descriptivo-correlacional. La conclusión a la que arriba el autor es que "los presupuestos especiales de los delitos informáticos permiten establecer una relación directa con la criminalidad económica, que no solamente se circunscribe a delitos patrimoniales, sino que también engloba tipos penales que cuentan con una importante repercusión en el sistema informático y, accesoriamente, en el sistema económico" (p. 108). Al respecto debemos señalar que en efecto los delitos informáticos no solo afectan el derecho a la autodeterminación informativa de las personas – ya que tienen por finalidad la sustracción de datos o información personal –; sino que también afectan sistema económico, en la medida de que con la información personal ilegalmente sustraída se suelen solicitar préstamos o realizar operaciones económicas suplantando la identidad de las personas agraviadas con estos delitos.

Sotomayor (2022) realizó un estudio cuyo objetivo principal fue "identificar de que forma la calificación fiscal establece parámetros para investigar los delitos informáticos en el Distrito Fiscal de Lima Centro, 2019 – 2020" (p. 5). La investigación tuvo un enfoque cualitativo, fue una investigación de tipo básica, con un diseño fenomenológico. La conclusión a la que arribó la autora es que "a través de la calificación fiscal que se realiza en las investigaciones relacionadas a delitos informáticos en el periodo analizado, se advierte que se no fueron los correctos para establecer como tal la existencia del delito investigado, tanto más si este se desnaturalizaba y se generaba otro delito al finalizar las investigaciones, por ejemplo se empezaba a calificar la noticia criminal como delito informático, pero se terminaba formalizando por hurto agravado". Al respecto debemos señalar que la deficiente formación y falta de capacitación de los operadores de justicia en materia de delitos informáticos, tiene por consecuencia que no se tenga una adecuada y eficaz persecución de estos delitos.

En lo correspondiente a los **Antecedentes Regionales o Locales**, tenemos a:

Rodríguez (2023) quien en su estudio que realizo tuvo por objetivo "dar paso en nuestro distrito judicial a la implementación, capacitación y ejecución en los diferentes órganos

encargados de la investigación y juzgamiento de los delitos informáticos en sus diferentes modalidades en la provincia de Ica, con una metodología de investigación de tipo básico y con un nivel explicativo; arribando a la conclusión que: Existe una conexión significativa entre los hurtos digitales y la falta de aplicación de la ley, los resultados muestran un valor crítico de 0,711, estos hallazgos coinciden con el estudio realizado por la Universidad Nacional Mayor de San Marcos, donde se concluye que la Ley de Delitos Informáticos tiene como objetivo prevenir y sancionar conductas ilegales que afectan sistemas informáticos, datos, secreto de comunicaciones, patrimonio, fe pública y libertad sexual mediante el uso de las TIC". (p. 81) Es fundamental recomendar que el Estado identifique con precisión el origen de los delitos informáticos y promueva políticas de ciberseguridad, especialmente en sectores vulnerables, comenzando por instituciones que resguardan información valiosa de distintos indoles, cuya vulneración afectaría gravemente el interés público y la seguridad nacional.

Vilela (2021) llevó a cabo una investigación cuyo objetivo "determinar como la información ya sea de administración pública, privada o personal dentro del ámbito informático pueden ser utilizados con el fin de la violación a la intimidad y utilizados de forma ilícita para la realización de actos delictivos" (p. 7). La investigación tuvo un enfoque cualitativo, siendo por su finalidad de tipo básica. La conclusión a la que arribó el autor es que "aquellos que no tienen estos conocimientos básicos de informática, son más propensos a convertirse en víctimas de delitos informáticos; esta parte de la población puede llegar a ser la parte más afectada y si en algún momento dado llegan a manejar un sistema informático y no se le ha dicho de manera adecuada que utilice la tecnología responsable del mismo conforme a la encuesta se deduce que se debe implementar mayor seguridad en las redes para que así los ciberdelincuentes no lo utilizarán y causarán graves daños económicos y psicológicos" (p.29). Al respecto debemos señalar que coincidimos con la conclusión del autor, en el sentido de que las personas que menor manejo tienen de la tecnología son las más propensas y las que por lo general son víctimas de los delitos informáticos.

En torno a las **Bases Teóricas** se tiene que:

Villavicencio (2014) señala que los delitos informáticos se encuentran relacionados con la perspectiva del crimen cometido a través de la computadora, internet, etc; no obstante, en forma de criminalidad no solo se realiza mediante la utilización de estos medios, en tanto que estos solo son instrumentos o herramientas que facilitan, pero no determinan la comisión de estos delitos. En tal sentido se define a la criminalidad informática como aquellas conductas que tienen por finalidad burlas los sistemas de seguridad, es decir, invasiones a computadoras,

correos o sistemas de datas mediante una clave de acceso; conductas que solo pueden ser cometidas a través de instrumentos o herramientas tecnológicas.

A su vez, Alcantara (2024) señala: “Al analizar la Ley 30096 sobre delitos informáticos y su aplicación frente al fraude cibernético en el país, se identificaron vacíos legales y deficiencias normativas. Se evidenció una regulación inadecuada por parte de los legisladores y una interpretación limitada de los operadores de justicia, requiriendo una reforma urgente”. (p.57).

Así también, Ramírez; Castro (2018) señalaron que el delito cibernético o informático "consiste en cualquier acto ilegal que se produce a través de medios informáticos o intentos de manipular o destruir computadoras, redes de Internet o medios electrónicos".

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

Por su parte Pardo (2018) es la investigación que realizó señala las principales características de los delitos cibernéticos, los mismo que a continuación se enumeran:

- **Es de carácter internacional**, estos delitos pueden ser cometidos desde cualquier parte del mundo.
- **El alcance judicial de estos delitos** es reducido, debido al escaso y reducido índice de denuncias, alcance regulatorio, falta de operadores de justicia especializados en materia de delitos informáticos.
- Por lo general, **son malintencionados o deliberados**, es decir son cometidos de forma dolosa.
- **Pueden ocasionar mucha corrupción económica grave**, porque por lo general se afectan grandes sumas de dinero o activos.
- Debido a sus especiales características técnicas, resulta compleja su probanza.
- Requiere de reducido espacio y tiempo, puesto que estos delitos se pueden se pueden realizar en pocos segundos o con un clic. Además, generalmente **no se requieren grandes equipos o máquinas informáticas** porque se puede realizar a través de un teléfono móvil de bolsillo.
- Estos **son comportamientos oportunistas**, debido a que quienes los comenten se benefician del rápido avance de la tecnología.

- **Estos son comportamientos profesionales**, y los ciberdelincuentes toman ventaja en su actuar delictivo en el ámbito de las victimas que hacen uso de los medios informáticos para trabajar.
- **Este es un delito de reciente aparición**.
- **Estos son delitos de cuello blanco**, solo puede cometerse por personas con conocimiento especializado en informática y tecnología de la información.

Con respecto al bien jurídico protegido en los delitos informáticos, Villavicencio (2014) refiere que ha de entenderse en los planos de manera conjunta y concatenada; en cuanto al primero se halla la información de forma general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos); y en lo que respecta al segundo plano, es estos delitos también se afectan bienes jurídicos como la indemnidad sexual, intimidad, etc. En lo referido a la información, esta debe ser entendida como el contenido de las bases y/o banco de datos el resultado de los procesos informáticos automatizados; por lo que, se trata de un bien con autonomía y valor económico. Siendo que es la importancia del valor económico de la que reviste la información, la que la convierte en bien jurídico tutelado.

Ahora, con respecto al phishing, Rojas (2024) señala "El phishing carece de una regulación específica en la normativa peruana y suele tratarse como estafa agravada, pese a ser una fase previa de varios delitos informáticos; resulta indispensable incorporar expresamente el phishing en el artículo 8° de la Ley N.° 30096, modificada por el Decreto Legislativo N.° 1614, ya sea como inciso independiente o mediante un párrafo específico. Esta incorporación evitaría interpretaciones subjetivas, permitiendo una persecución penal más clara y eficaz, reconociendo al phishing como un ilícito digital autónomo. De este modo, se brindaría mayor protección a las víctimas y se fortalecería la respuesta del sistema de justicia ante las amenazas de la ciberdelincuencia". (p.99).

Así también: el phishing, en particular, es un tipo de engaño que consiste en el envío de comunicaciones con apariencia de ser legítimas, pero que en realidad son falsas y buscan convencer a que la víctima realice determinadas acciones; lo que puede incluir presionar un clic en un enlace misterioso, descargar un archivo con virus o introducir información sensible en un sitio web falso que parece uno legítimo (Van Dijk; Van Deursen, 2014).

Por otro lado, Akbari, et.al. (2024) señala que "el phishing y los engaños en el ámbito digital son técnicas cada vez más sofisticadas utilizadas por los ciberdelincuentes para obtener información confidencial de manera fraudulenta". Este tipo de acciones se basan en la manipulación psicológica y la ingeniería social, con la finalidad de lograr la confianza de las

víctimas y a veces aprovecharse de su descuido o ignorancia para engañarlos y lograr que divulguen sus datos personales.

Entonces, “la efectividad del phishing y otros engaños radica en su capacidad para generar un sentido de urgencia o miedo, presionando a las víctimas para que actúen rápidamente y sin cuestionar la legitimidad de la solicitud” (Ayuso García; Ayuso Sánchez, 2010). Por ejemplo, un ataque de phishing puede simular una alerta de seguridad crítica o una notificación de acceso no autorizado a una cuenta, instando al usuario a "confirmar" su identidad o "verificar" su información de inmediato (Akbari, et al, 2024).

Así también se dice que el phishing “es una técnica común utilizada por los ciberdelincuentes para engañar a las personas y obtener información confidencial, como contraseñas y detalles financieros. Este método implica el envío de correos electrónicos o mensajes que parecen legítimos pero que en realidad son fraudulentos” (Hamdi, et al, 2021).

El phishing, por otro lado, “se basa en la ingeniería social para engañar a las personas y obtener información confidencial, como contraseñas y detalles financieros. Los ataques de phishing han evolucionado para ser cada vez más sofisticados y específicos, utilizando técnicas como el spear phishing para dirigirse a individuos concretos dentro de una organización. La educación y concienciación de los usuarios son esenciales para combatir este tipo de amenaza, así como el desarrollo de tecnologías avanzadas de filtrado y detección de correos electrónicos maliciosos” (Fu Wang; Feng, 2024)

Es así que, uno de los retos más importantes es el ritmo acelerado de la evolución tecnológica siendo que, el surgimiento de nuevas tecnologías como la inteligencia artificial, la biometría, y las redes sociales ha cambiado el escenario del crimen y en consecuencia las estrategias necesarias para combatirlo (Aguirre; Jiménez, 2020). “La ciberdelincuencia, por ejemplo, plantea problemas particulares en términos de jurisdicción y extraterritorialidad, ya que los delitos pueden cometerse desde cualquier lugar del mundo, dificultando la identificación y persecución de los infractores (Roztocki; Sojas; Roland, 2019).

En respuesta a estos desafíos, resulta de vital importancia promover la innovación y adaptabilidad del marco normativo a las nuevas tecnologías u metodologías, la formación contante de los operadores de justicia, y la elaboración de leyes que colaboren a combatir eficientemente a las cambiantes dinámicas del crimen y la justicia, más aún si se está frente a delitos informáticos o ciberdelitos (Tavares; Bitencourt, 2021).

“Así que, combatir el phishing y los engaños requiere una combinación de medidas técnicas, educativas y de políticas. A nivel individual, es crucial desarrollar una mentalidad crítica y verificar siempre la autenticidad de las comunicaciones recibidas, especialmente si solicitan información sensible” (Añasco, Morocho; Hallo, 2023).

En relación al fraude informático, el “Artículo 8 de la Ley 30096” dispone que, mediante tecnologías de la información y comunicación, si alguien obtiene un beneficio ilegal para sí mismo o para otros, a través del diseño, acceso, modificación, eliminación, interrupción o duplicación de datos informáticos, puede ser condenado a una pena de prisión que va de 3 a 8 años, además de una multa de 70 a 120 días. Este mismo artículo contempla una agravante que establece una pena de prisión de 5 a 10 años y una multa de 80 a 140 días, cuando se afectan propiedades del Estado reservadas para el sostenimiento de ayudas a los más necesitados. Asimismo, en el convenio sobre ciberdelincuencia, que entró en vigor en diciembre de 2019, se establece en el artículo 8 que los gobiernos firmantes deben promover iniciativas legislativas que busquen prevenir, intervenir y sancionar a quienes cometen delitos en internet, perpetrados por personas que laboran en distintos países.

El fraude informático se define como una manera ilegal de obtener beneficios mediante la manipulación de datos almacenados en dispositivos electrónico (Jiménez, 2017). Con el aumento de transacciones digitales en 2020 y 2021, surge una mayor actividad delictiva en internet. Arias (2021) identifica tres aspectos criminológicos del fenómeno: “el riesgo asociado al conocimiento y el desarrollo de sistemas informáticos, el peligro del uso indebido de la información en una sociedad competitiva, el daño significativo que el abuso informático causa a las víctimas”.

Tambien, se toma en cuenta lo expuesto por Bravo (2024) quien señala “En los últimos años, el fraude informático ha aumentado considerablemente, convirtiéndose en una de las principales amenazas para la economía y la seguridad digital en el Perú. Este crecimiento está ligado al uso masivo de internet y plataformas digitales, que han transformado las dinámicas comerciales, sociales y financieras. No obstante, el fácil acceso a la tecnología ha facilitado el surgimiento de nuevas formas delictivas que perjudican a ciudadanos, empresas e instituciones; la escasa cultura de ciberseguridad y la limitada formación digital en la población han favorecido la recurrencia de estos delitos, generando inseguridad y desconfianza en el entorno virtual” (p.54).

Asimismo, Rivera (2025) señala que “El Estado peruano cumple una función fundamental en la prevención de los delitos informáticos, aunque requiere seguir reforzando su legislación, capacitar a sus funcionarios y promover la cooperación nacional e internacional. Asimismo,

educar y sensibilizar a la ciudadanía resulta esencial para prevenir estos crímenes y fortalecer la ciberseguridad del país" (p.43).

La Tesis "LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024" demuestra la relación entre las variables motivo de estudio.

El **Problema General fue:** ¿De qué manera los delitos informáticos suponen un desafío para la regulación penal en el Distrito Fiscal de Ica, año 2024?; En lo que respecta a **los Problemas Específicos** tenemos: **Problema Específico 1:** ¿Cómo influye el incremento del delito de phishing en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024?; **Problema Específico 2:** ¿Qué impacto tiene la incidencia del fraude informático en las limitaciones del marco normativo penal en el Distrito Fiscal de Ica, año 2024?

La investigación realizada se **justifica legalmente** porque ha tomado en consideración: la Constitución Política del Perú de 1993; la Ley N.º 30220, Ley Universitaria; el Estatuto de la Universidad Nacional San Luis Gonzaga (UNICA); la Resolución Rectoral N.º 029-2021-R, que establece las Líneas de Investigación de la UNICA; la Resolución Rectoral N.º 048-2021-R, correspondiente al Reglamento de Grados y Títulos; y la Resolución Rectoral N.º 1320-2021-R, que aprueba la Guía para la Elaboración de Proyecto de Tesis y Tesis. Asimismo, el Código Penal, Código Procesal Penal, Ley Nº 30096 - Ley de Delitos Informáticos; Ley 32314: modifican el Código Penal y otro para sancionar el uso de la inteligencia artificial en la comisión de delitos; entre otros. Estas normas y disposiciones constituyen el marco normativo que respalda y orienta el desarrollo de la presente investigación.

En lo que se refiere a la **Justificación Teórica,** la presente investigación se justifica en la necesidad de comprender los desafíos que representan los delitos informáticos para el sistema penal, particularmente en el Distrito Fiscal de Ica. En un contexto donde la tecnología avanza a ritmo acelerado, el marco normativo y las capacidades institucionales no siempre logran adaptarse con la misma velocidad, generando vacíos legales, dificultades probatorias y limitaciones en la persecución penal efectiva; en lo que respecta a la **Justificación Práctica** la investigación realizada, la misma es de gran de gran utilidad para fiscales, jueces, abogados penalistas, policías de la DIVINCRI y ciudadanía en general, al ofrecer un diagnóstico claro sobre cómo los delitos informáticos desafían la actual regulación penal en el Distrito Fiscal de Ica. Los resultados permiten a las autoridades identificar vacíos normativos, deficiencias en la

capacitación técnica y limitaciones operativas que obstaculizan la persecución eficaz de este tipo de criminalidad. Asimismo, proporcionan una base empírica para tomar decisiones informadas, fortalecer políticas públicas, mejorar protocolos de actuación y promover reformas normativas y estructurales que contribuyan a una respuesta penal más eficiente y adaptada al entorno digital. De este modo, se busca fortalecer la lucha contra el crimen informático, mejorando la seguridad jurídica y tecnológica en la región; en cuanto a la **Justificación Metodológica,** la metodología empleada en esta investigación, de tipo básica y nivel explicativo, con diseño correlacional, que permite analizar las relaciones entre las variables jurídicas de manera objetiva y estructurada, facilitando la comprensión de fenómenos interdependientes. La elección de este enfoque responde a la necesidad de describir y explicar comportamientos jurídicos sin intervenir directamente sobre ellos. Asimismo, se desarrollaron instrumentos como encuestas, aplicadas a una muestra representativa de la población objeto de estudio, lo que permitió una recolección precisa de datos. Esto contribuye significativamente a la validez de los resultados y sirve como base para futuras investigaciones en el ámbito jurídico.

La importancia de la investigación radica en el incremento exponencial de conductas delictivas que se cometen a través de medios digitales, lo cual representa un serio reto para la administración de justicia penal. En ese sentido, donde la tecnología avanza más rápido que la normativa, se hace imprescindible estudiar la eficacia del marco jurídico actual, la preparación de los operadores del sistema penal y la capacidad institucional para enfrentar estos nuevos delitos. Con esta investigación se buscó identificar las deficiencias normativas y procedimentales que obstaculizan la correcta persecución y sanción de los delitos informáticos, proponiendo soluciones viables desde una perspectiva jurídico-penal. La investigación se desarrolló en el Distrito Fiscal de Ica durante el año 2024, considerando esta jurisdicción como un espacio representativo para analizar el impacto real de la criminalidad digital en el ámbito regional. Se utilizó una metodología de tipo descriptivo-correlacional, con enfoque cuantitativo, a fin de obtener una visión integral del fenómeno. Los resultados permiten aportar al fortalecimiento del sistema penal y ofrecer herramientas útiles a fiscales, jueces, policías especializados y legisladores para enfrentar los desafíos que impone la era digital.

El **Objetivo General** fue: Analizar de qué manera los delitos informáticos suponen un desafío para la regulación penal en el Distrito Fiscal de Ica, año 2024. Los **Objetivos Específicos** fueron: **Objetivo Específico 1**: Establecer cómo el incremento del delito de phishing influye en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024; **Objetivo Específico 2**: Determinar el impacto de la incidencia del fraude informático en las limitaciones del marco normativo penal en el Distrito Fiscal de Ica, año 2024.

La **Hipótesis General** fue: Los delitos informáticos constituyen un desafío creciente para la regulación penal en el Distrito Fiscal de Ica, debido a su constante evolución tecnológica y limitada adaptación normativa, en el año 2024. **Las Hipótesis Específicas** fueron: **Hipótesis Específica 1:** El incremento del delito de phishing influye negativamente en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024. **Hipótesis Específica 2:** La continua incidencia del fraude informático evidencia las limitaciones del marco normativo penal, reduciendo su eficacia frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024.

Las Variables fueron:

Variable Independiente (X): **Delitos informáticos.**

Flores (2014) señala que los delitos informáticos pueden definirse como cualquier acción u omisión que está legalmente tipificada y sancionada con una pena, y son llevados a cabo por una persona en el ámbito de la informática, con la consecuencia de causar perjuicio a individuos específicos y proporcionar beneficios ilícitos al autor del delito.

Dimensiones:

Phishing.

Fraude informático.

Variable Dependiente (Y): **Regulación penal en la era digital.**

De acuerdo con Fernández (2024) El derecho penal y procesal penal están experimentando una profunda transformación en la era digital, lo cual merece un tratamiento serio y responsable para hacer frente a los retos y desafíos contemporáneos. Por eso, es importante gestionar y fortalecer las competencias del profesional en la disciplina jurídica; además, para ampliar sus conocimientos, mejorar la asesoría y optimizar el patrocinio se debe perfeccionar la técnica jurídica, proponer la adaptación de las leyes a la complejidad de la criminalidad.

Dimensiones:

Capacidad

Eficacia

Operacionalización de Variables:

La Matriz de Operacionalización se presenta en la Parte de Anexos.

II. ESTRATEGIA METODOLÓGICA

2.1. TIPO, NIVEL Y DISEÑO DE INVESTIGACIÓN

2.1.1. TIPO DE INVESTIGACIÓN:

Por su finalidad, “el estudio se enmarcó en una investigación de tipo básica, ya que, buscó contribuir al desarrollo teórico y una ampliación del conocimiento relacionado con las variables analizadas, es decir, analizar de qué manera los delitos informáticos suponen un desafío para la regulación penal en el Distrito Fiscal de Ica, año 2024”.

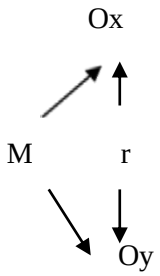
2.1.2. NIVEL DE INVESTIGACIÓN:

De acuerdo a la naturaleza del estudio de la investigación, “reúne por su nivel las características de un estudio correlacional, ya que permitió identificar la relación existente entre las variables planteadas en el estudio (Los delitos informáticos y la regulación penal: Un análisis de los nuevos desafíos en la era digital), sin necesidad de establecer una causalidad directa, pero sí evidenciando patrones y vínculos significativos”.

2.1.3. DISEÑO DE INVESTIGACIÓN:

El diseño metodológico de la presente investigación es no experimental y transversal.

Se clasifica como no experimental porque las variables han sido observadas y analizadas en su contexto natural, sin manipulación deliberada por parte del investigador, permitiendo evaluar su incidencia e interrelación tal como se presentan en la realidad. Asimismo, se considera transversal o transeccional, dado que la recolección de datos se ha realizado en un periodo puntual (2024) y dentro de un espacio determinado (Distrito fiscal de Ica). Por la naturaleza del estudio, este se ubica dentro de los diseños descriptivos, y específicamente dentro del diseño correlacional, al buscar establecer la relación entre las variables investigadas. En consecuencia, el diseño está compuesto por el siguiente esquema metodológico:



En donde:

M: Fiscales, jueces, abogados penalistas, policías de la DIVINCRI y público en general.

Ox: Delitos Informáticos.

Oy: Regulación penal en la era digital.

r: Factor de correlación.

2.2. POBLACIÓN, MUESTRA Y MUESTREO

2.2.1. POBLACIÓN

Según Monje (2011), "la población —también conocida como universo— corresponde al conjunto de elementos, unidades u objetos que poseen características similares relacionadas con la investigación, y cuyos resultados pueden ser deducidos a partir del análisis de una muestra" (p. 26).

En este contexto, ***"la población objeto de estudio en la presente investigación estuvo conformada por 100 colaboradores entre fiscales, jueces, abogados penalistas, policías de la DIVINCRI y público en general del Distrito Fiscal de Ica*"**.

N=100

2.2.2. MUESTRA

La muestra representa una sección de la población que la simboliza; "es una pequeña porción que puede indicar el estado del objeto de estudio. Por ejemplo, en un análisis clínico, basta con extraer una gota de sangre del paciente para examinar y conocer su estado de salud" (Sánchez, 2019).

Así también, se puede decir que la muestra "es una parte representativa del conjunto del total de la población en estudio, a partir de la cual se recogen los datos que serán examinados en el contexto de la investigación. Su selección se basa en criterios metodológicos que aseguran la validez y confiabilidad de los datos obtenidos. En esta investigación, la muestra estuvo conformada por 80 colaboradores, quienes fueron seleccionados por reunir las características relevantes al fenómeno en estudio, lo que garantizó su representatividad respecto a la población total, como se muestra en el siguiente cuadro":

Distribución de la Muestra

Cargo	N º de individuos
Fiscales	4
Jueces	4
Abogados penalistas	12
Policías de la DIVINCRI	25
Público en general	35
Total	**80**

La muestra se determinó aplicando la siguiente fórmula estadística:

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{E^2 \cdot (N-1) + Z^2 \cdot p \cdot (1-p)}$$

$$80 = \frac{N \cdot (1.96)^2 \cdot 0.5 \cdot 0.5}{(0.05)^2 \cdot (N-1) + (1.96)^2 \cdot 0.5 \cdot 0.5}$$

Donde: n= Tamaño de la muestra; N= Tamaño total de la población; Z= Nivel de confianza; p= Variabilidad positiva o probabilidad de éxito; **y** E= Margen de error o precisión

2.2.3. MUESTREO

Según la literatura especializada, existen dos tipos de muestreo; uno probabilístico y otro no probabilístico. “En el muestreo probabilístico, cualquier individuo que forma parte de la población puede ser seleccionado, pero que en su conjunto representa a toda la población; siempre y cuando la representatividad debe de encontrarse en un numero estadístico mínimo de personas u objetos que representen a la población con un margen de error que se acepta. Por otro lado, en el muestreo no probabilístico se extraen a los participantes de la muestra, atendiendo a la consideraciones o criterios que tenga el investigador diferente al azar, es decir, los componentes de la muestra no se eligen de forma aleatoria” (Sánchez, 2019).

En la presente se aplicó un muestreo un muestreo no probabilístico de tipo intencional, ya que la elección de los participantes se basó en una decisión consciente del investigador, quien los seleccionó considerando su relevancia y relación directa con el tema de estudio.

2.3. TÉCNICA E INSTRUMENTO DE INVESTIGACIÓN

2.3.1. TECNICA DE RECOLECCIÓN DE DATOS:

"Para la recopilación de datos se utilizó la técnica de la encuesta, por su factibilidad para la obtención de información pertinente y útil para los fines del estudio. Para ello, se elaboró un cuestionario con preguntas formuladas por el investigador, el cual fue entregado a los participantes para que lo respondan de forma individual y anónima"

Según Sánchez (2019), "la técnica de la encuesta se basa en recoger datos de un grupo de personas a las que se les proporciona un cuestionario que deben completar en un tiempo específico. El investigador puede ser el autor del instrumento o no, y su aplicación puede ser realizada por cualquier persona o a través de diferentes medios".

2.3.2. INSTRUMENTOS DE RECOLECCIÓN DE DATOS:

"El instrumento que se utilizó en esta investigación consta de cuestionarios estructurados, elaborados con el objetivo de recoger información vinculada a ambas variables: delitos informáticos y su regulación penal en la era digital. Para cada variable se desarrolló un cuestionario distinto, compuesto por 10 ítems con respuestas cerradas de tipo dicotómico, organizadas en una escala nominal".

Según señala Sánchez (2019), el cuestionario es "un instrumento que mide las opiniones o conocimientos de una persona o conjunto de personas por medio de preguntas o reactivos que han sido elaborados en relación a la variables, indicadores y objetivos de la investigación".

III. RESULTADOS

VARIABLE X: DELITOS INFORMÁTICOS

Dimensión: Phishing

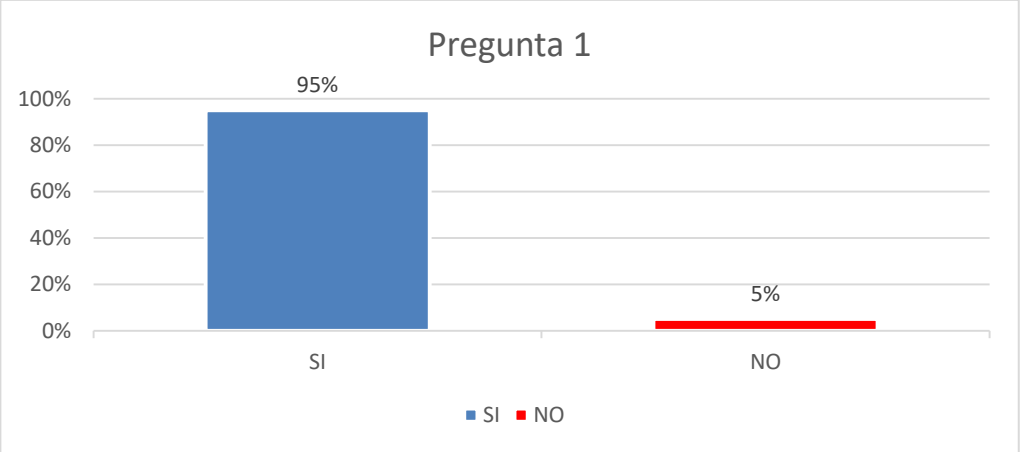
Tabla I.

P1: ¿Considera que el phishing es actualmente uno de los delitos informáticos más frecuentes?

	Frecuencia	Porcentaje
SI	76	95%
NO	4	5%
Total	80	100%

Fuente: Data de resultados

Figura 1



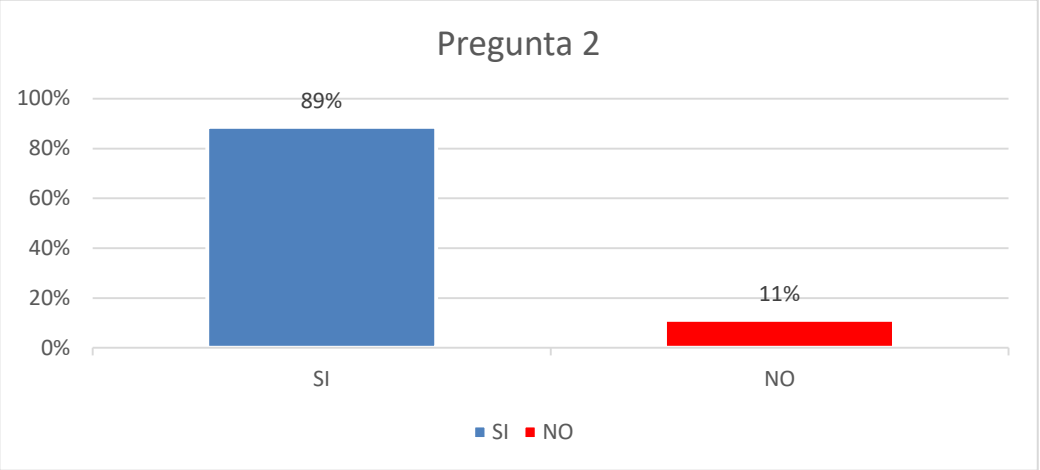
Interpretación: En la Tabla I, Figura 1, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión phishing, donde el 95% de los encuestados considera que el phishing es actualmente uno de los delitos informáticos más frecuentes, mientras que el 5% manifiesta no compartir dicha percepción. Estos resultados evidencian una elevada conciencia sobre la recurrencia de este tipo de delito, permitiendo identificar al phishing como una de las principales amenazas en el entorno digital actual. Asimismo, esta alta percepción de frecuencia refleja el nivel de exposición de la población frente a prácticas fraudulentas orientadas a la obtención ilícita de información personal, financiera o confidencial. Resulta pertinente destacar que la prevalencia del phishing no solo compromete la seguridad de los datos y sistemas informáticos, sino que también genera desconfianza en el uso de plataformas digitales, afectando el ejercicio seguro de derechos y el normal desarrollo de actividades personales, comerciales e institucionales.

Tabla II.

P2: ¿Ha observado un aumento en las denuncias por phishing en los últimos años?		
	Frecuencia	Porcentaje
SI	71	89%
NO	9	11%
Total	80	100 %

Fuente: Data de resultados

Figura 2



Interpretación:

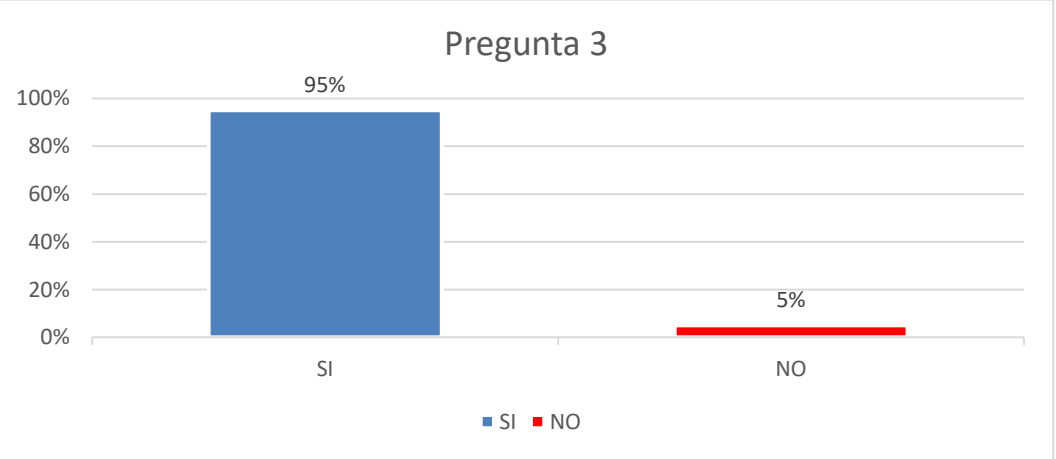
En la Tabla II, Figura 2, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión phishing, donde el 89% de los encuestados manifiesta haber observado un aumento en las denuncias por phishing en los últimos años, mientras que el 11% indica no haber percibido dicho incremento. Estos datos permiten identificar que el phishing se viene consolidando como un delito informático en constante crecimiento, evidenciando su mayor incidencia y visibilidad en el contexto actual. Resulta relevante destacar que este incremento en las denuncias no solo refleja una mayor ocurrencia de este tipo de conductas delictivas, sino también una creciente preocupación social frente a los riesgos que implica para la seguridad de la información y el patrimonio de las personas. Asimismo, el aumento del phishing afecta la confianza en los sistemas digitales y vulnera derechos fundamentales como la seguridad, la privacidad y la protección de los datos personales.

Tabla III

P3 ¿Está de acuerdo en que el phishing debe considerarse un delito grave dentro del Código Penal peruano?		
	Frecuencia	Porcentaje
SI	76	95%
NO	4	5%
Total	80	100%

Fuente: Data de resultados

Figura 3



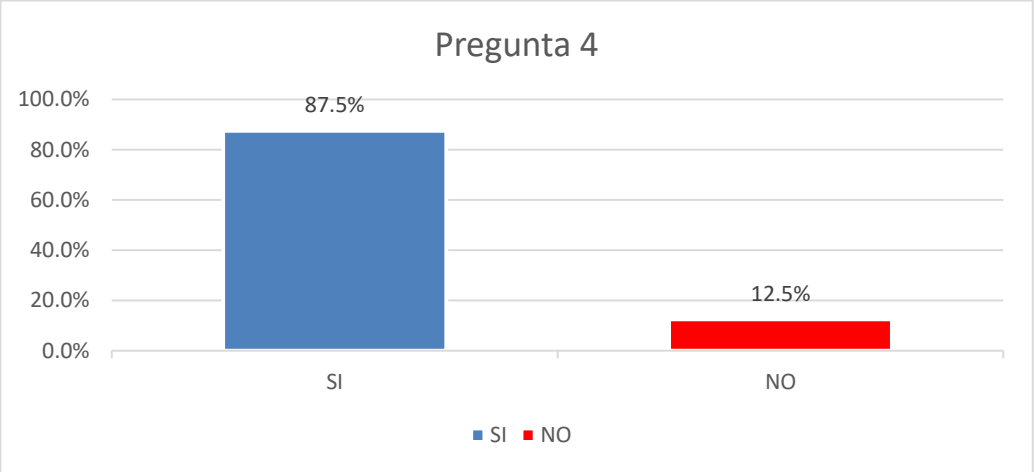
Interpretación: En la Tabla III, Figura 3, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión phishing, donde el 95% de los encuestados manifiesta estar de acuerdo en que el phishing debe considerarse un delito grave dentro del Código Penal peruano, mientras que el 5% indica no estar de acuerdo con dicha afirmación. Estos resultados permiten identificar una clara percepción social sobre la gravedad del phishing y el impacto perjudicial que genera en las personas y en la seguridad digital. Resulta relevante destacar que esta alta valoración de gravedad refleja la necesidad de un tratamiento penal más riguroso frente a estas conductas, en tanto el phishing no solo ocasiona perjuicios económicos, sino que también vulnera derechos fundamentales como la seguridad, la privacidad y la protección de los datos personales. Asimismo, la consideración del phishing como delito grave evidencia la demanda de una respuesta normativa eficaz que contribuya a la prevención, sanción y reducción de este tipo de delitos en el contexto peruano.

Tabla IV.

P4 ¿Ha recibido usted o alguien de su entorno correos electrónicos sospechosos solicitando datos personales?		
	Frecuencia	Porcentaje
SI	70	87.5%
NO	10	12.5%
Total	80	100%

Fuente: Data de resultados

Figura 4



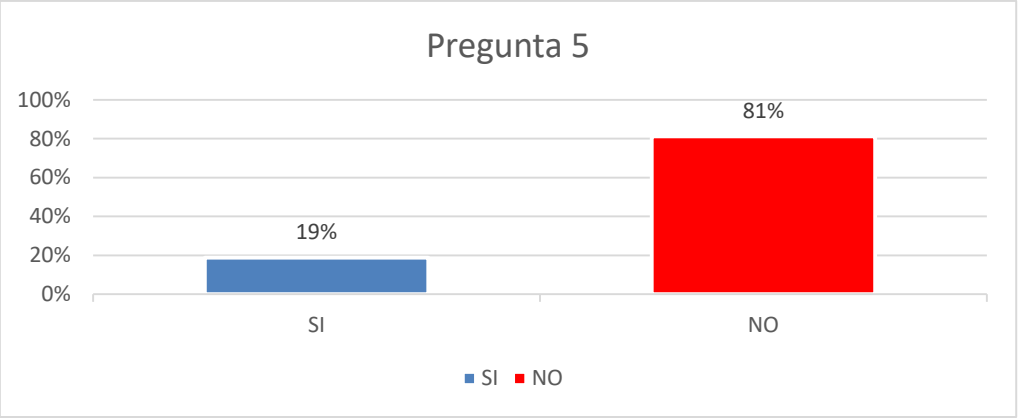
Interpretación: En la Tabla IV, Figura 4, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión phishing, donde el 87,5% de los encuestados manifiesta haber recibido, ya sea personalmente o a través de alguien de su entorno, correos electrónicos sospechosos que solicitan datos personales, mientras que el 12,5% indica no haber tenido este tipo de experiencia. Estos datos permiten identificar que la recepción de mensajes fraudulentos vinculados al phishing constituye una práctica frecuente en el entorno digital actual, evidenciando la amplia difusión y alcance de este delito informático. Resulta relevante destacar que estas acciones no solo representan un riesgo significativo para la seguridad de la información y el patrimonio de las personas, sino que también vulneran derechos fundamentales como la privacidad, la seguridad y la protección de los datos personales, generando además desconfianza en el uso de los medios electrónicos y plataformas digitales.

Tabla V.

P5 ¿Cree que los bancos y entidades financieras están aplicando medidas efectivas contra el phishing?		
	Frecuencia	Porcentaje
SI	15	19%
NO	65	81%
Total	80	100%

Fuente: Data de resultados

Figura 5



Interpretación: En la Tabla V, Figura 5, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión phishing, donde solo el 19% de los encuestados considera que los bancos y entidades financieras están aplicando medidas efectivas contra el phishing, mientras que el 81% manifiesta que dichas medidas no resultan suficientes. Estos datos permiten identificar una percepción mayoritaria de ineficacia en las acciones implementadas por las entidades financieras frente a este delito informático, lo que evidencia un escenario de vulnerabilidad para los usuarios del sistema financiero. Resulta relevante destacar que esta percepción negativa no solo refleja una falta de confianza en los mecanismos de prevención y seguridad adoptados por las instituciones bancarias, sino que también incrementa el riesgo de afectación al patrimonio económico de las personas. Asimismo, la insuficiencia de medidas efectivas contra el phishing compromete derechos fundamentales como la seguridad, la protección de los datos personales y la confianza en los servicios financieros digitales.

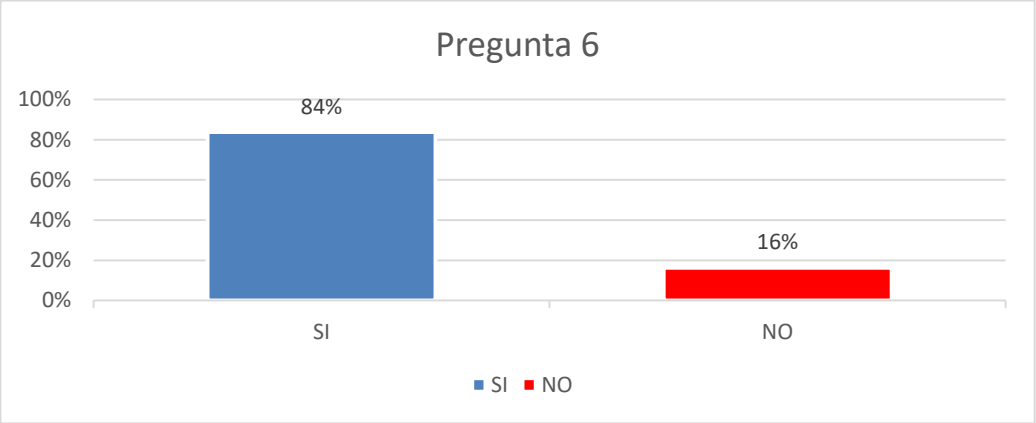
Dimensión: Fraude informático

Tabla VI.

P6 ¿Cree usted que el fraude informático se ha convertido en uno de los delitos más comunes en el ámbito digital?		
	Frecuencia	Porcentaje
SI	67	84%
NO	13	16%
Total	80	100%

Fuente: Data de resultados

Figura 6



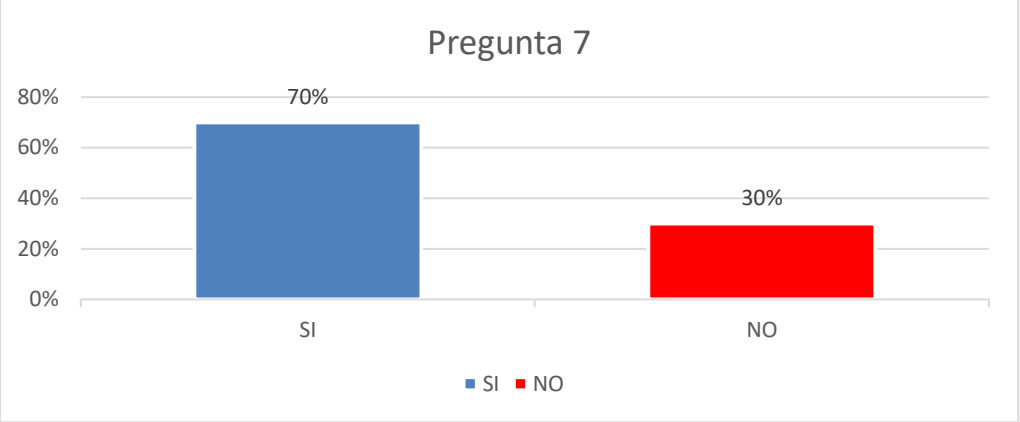
Interpretación: En la Tabla VI, Figura 6, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión fraude informático, donde el 84% de los encuestados considera que el fraude informático se ha convertido en uno de los delitos más comunes en el ámbito digital, mientras que el 16% manifiesta no compartir dicha percepción. Estos datos permiten identificar que el fraude informático es percibido como una práctica recurrente en el entorno digital actual, evidenciando su creciente incidencia y alcance. Resulta relevante destacar que la frecuencia de este tipo de delitos no solo afecta la seguridad de los sistemas informáticos, sino que también genera consecuencias negativas de carácter económico y social, vulnerando derechos fundamentales como la seguridad, la integridad patrimonial y la protección de los datos personales. Asimismo, la percepción de su alta ocurrencia pone de manifiesto la necesidad de fortalecer las estrategias de prevención, control y sanción frente a estas conductas ilícitas en el ámbito digital.

Tabla VII.

P7 ¿Conoce casos cercanos de personas afectadas por fraudes informáticos?		
	Frecuencia	Porcentaje
SI	56	70%
NO	24	30%
Total	80	100%

Fuente: Data de resultados

Figura 7



Interpretación: En la Tabla VII, Figura 7, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión fraude informático, donde el 70% de los encuestados manifiesta conocer casos cercanos de personas afectadas por fraudes informáticos, mientras que el 30% indica no tener conocimiento de este tipo de situaciones. Estos datos permiten identificar que el fraude informático constituye una problemática cercana y presente en el entorno social de los participantes, evidenciando su impacto directo en la vida cotidiana de las personas. Resulta relevante destacar que la cercanía de estos casos no solo refleja la frecuencia con la que se presentan este tipo de delitos, sino que también pone de manifiesto las consecuencias negativas que generan, principalmente en el ámbito económico y emocional de las víctimas. Asimismo, los fraudes informáticos vulneran derechos fundamentales como la seguridad, la protección de los datos personales y la integridad patrimonial, afectando la confianza en el uso de los medios y servicios digitales.

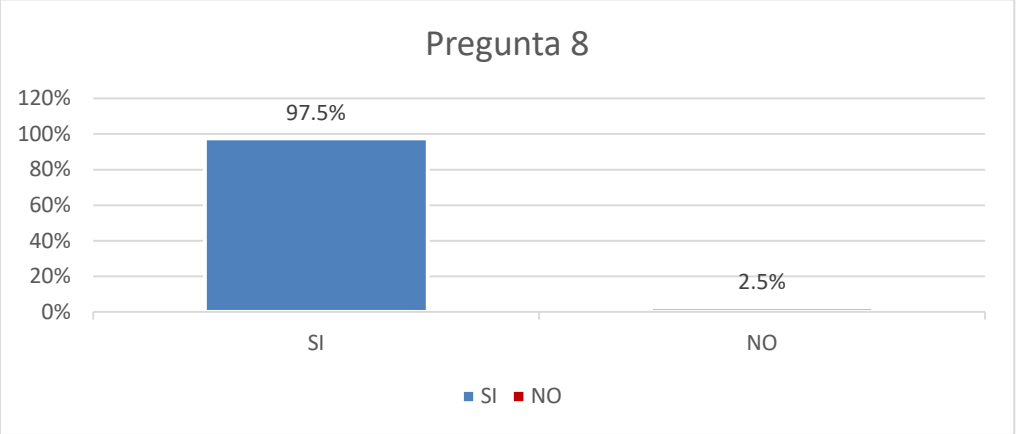
Tabla VIII.

P8 ¿Considera que los delincuentes informáticos actúan con mayor frecuencia aprovechando el desconocimiento de los usuarios?		
	Frecuencia	Porcentaje

SI	78	97.5%
NO	2	2.5%
Total	80	100 %

Fuente: Data de resultados

Figura 8



Interpretación: En la Tabla VIII, Figura 8, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión fraude informático, donde el 97,5% de los encuestados considera que los delincuentes informáticos actúan con mayor frecuencia aprovechando el desconocimiento de los usuarios, mientras que solo el 2,5% manifiesta no estar de acuerdo con dicha afirmación. Estos datos permiten identificar que el desconocimiento de los usuarios constituye un factor determinante que facilita la comisión de fraudes informáticos, evidenciando una situación de alta vulnerabilidad en el entorno digital. Resulta relevante destacar que esta condición no solo incrementa la probabilidad de que las personas sean víctimas de este tipo de delitos, sino que también pone en riesgo derechos fundamentales como la seguridad, la privacidad y la protección de los datos personales. Asimismo, la elevada percepción sobre el aprovechamiento del desconocimiento resalta la necesidad de fortalecer la educación digital y las estrategias de prevención como mecanismos clave para reducir la incidencia del fraude informático.

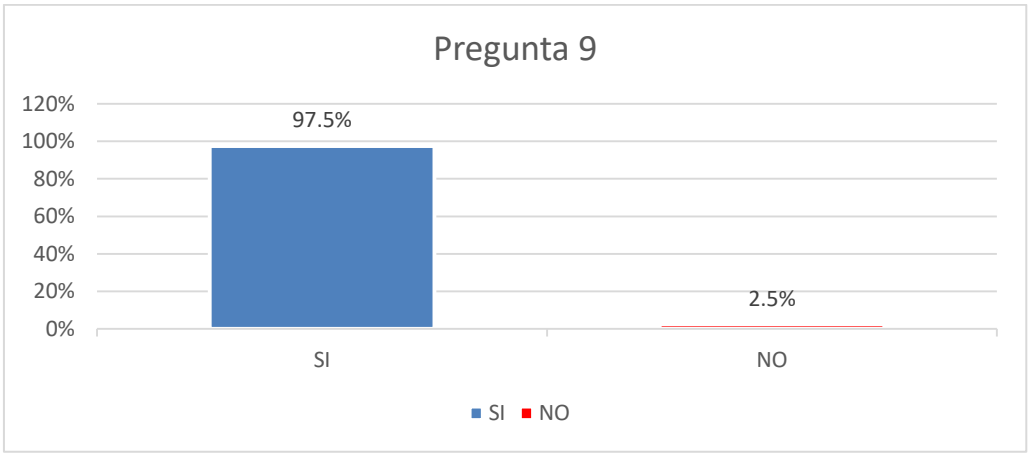
Tabla IX.

P9 ¿Piensa que los fraudes informáticos están aumentando debido al fácil acceso a herramientas tecnológicas?		
	Frecuencia	Porcentaje
SI	78	97.5%

NO	2	2.5%
Total	80	100%

Fuente: Data de resultados

Figura 9



Interpretación: En la Tabla IX, Figura 9, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión fraude informático, donde el 97,5% de los encuestados considera que los fraudes informáticos están aumentando debido al fácil acceso a herramientas tecnológicas, mientras que solo el 2,5% manifiesta una opinión contraria. Estos datos permiten identificar que la disponibilidad y accesibilidad de herramientas tecnológicas constituye un factor determinante en el incremento de los fraudes informáticos, favoreciendo la comisión de este tipo de delitos en el entorno digital. Resulta relevante destacar que este escenario no solo incrementa la incidencia de conductas ilícitas, sino que también intensifica los riesgos para la seguridad de la información, el patrimonio económico y la privacidad de los usuarios. Asimismo, el aumento de los fraudes informáticos vulnera derechos fundamentales como la seguridad, la protección de los datos personales y la integridad patrimonial, evidenciando la necesidad de reforzar las políticas de control, prevención y regulación en el uso de tecnologías digitales.

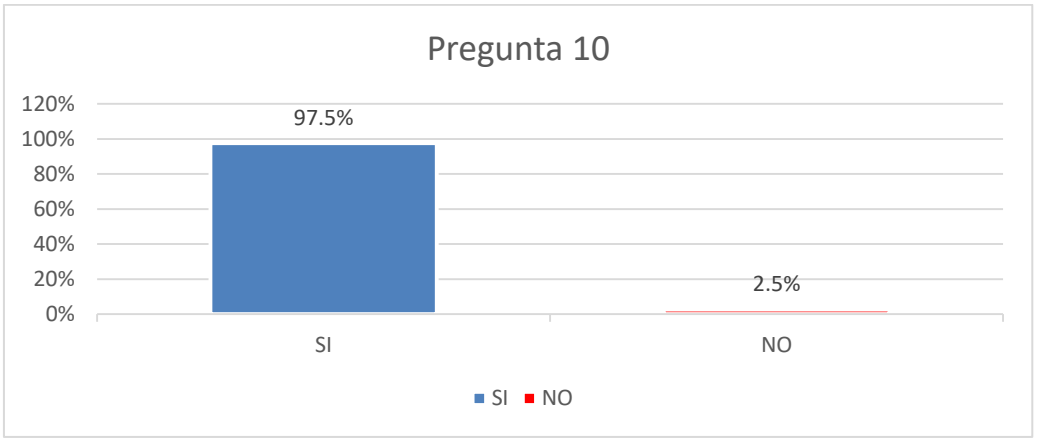
Tabla X.

P10 ¿Considera que las redes sociales son un canal frecuente para la comisión de fraudes informáticos?		
	Frecuencia	Porcentaje
SI	78	97.5%

NO	2	2.5%
Total	80	100,00%

Fuente: Data de resultados

Figura 10



Interpretación: En la Tabla X, Figura 10, se presentan las respuestas de los 80 participantes respecto a la variable delitos informáticos, en la dimensión fraude informático, donde el 97,5% de los encuestados considera que las redes sociales constituyen un canal frecuente para la comisión de fraudes informáticos, mientras que el 2,5% manifiesta no compartir dicha percepción. Estos datos permiten identificar que las redes sociales se han convertido en un medio recurrente utilizado por los delincuentes informáticos para ejecutar fraudes, aprovechando su amplio alcance, inmediatez y la interacción constante entre los usuarios. Resulta relevante destacar que el uso de las redes sociales como canal para estas conductas ilícitas no solo incrementa la probabilidad de que las personas sean víctimas de fraude, sino que también expone información sensible, vulnerando derechos fundamentales como la seguridad, la privacidad y la protección de los datos personales. Asimismo, esta situación evidencia la necesidad de fortalecer las medidas de prevención, control y educación digital orientadas al uso seguro de las plataformas sociales.

VARIABLE Y: REGULACIÓN PENAL EN LA ERA DIGITAL

Dimensión: Capacidad

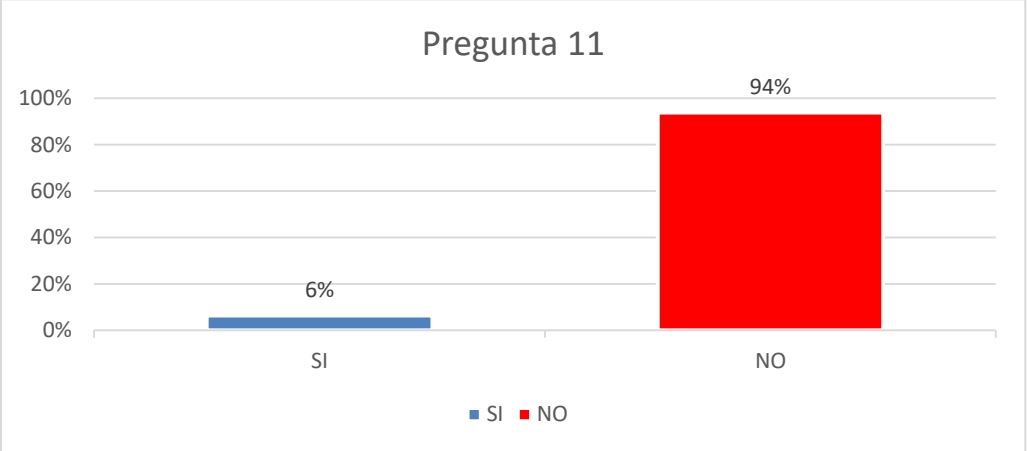
Tabla XI.

P11 ¿Piensa que el sistema penal tiene suficientes herramientas tecnológicas para enfrentar el cibercrimen?

	Frecuencia	Porcentaje
SI	5	6%
NO	75	94%
Total	80	100 %

Fuente: Data de resultados

Figura 11



Interpretación: En la Tabla XI, Figura 11, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión capacidad, donde solo el 6% de los encuestados considera que el sistema penal cuenta con suficientes herramientas tecnológicas para enfrentar el cibercrimen, mientras que el 94% manifiesta que dichas herramientas resultan insuficientes. Estos datos permiten identificar una percepción mayoritaria de debilidad en la capacidad tecnológica del sistema penal frente a los desafíos que plantea la criminalidad digital. Resulta relevante destacar que está limitada capacidad tecnológica no solo dificulta la investigación, persecución y sanción de los delitos informáticos, sino que también genera un escenario de impunidad que afecta la confianza ciudadana en el sistema de justicia. Asimismo, la carencia de herramientas adecuadas compromete la protección efectiva de derechos fundamentales como la seguridad, la integridad patrimonial y la tutela jurisdiccional efectiva, evidenciando la necesidad de fortalecer la infraestructura tecnológica y las competencias especializadas del sistema penal en el contexto digital.

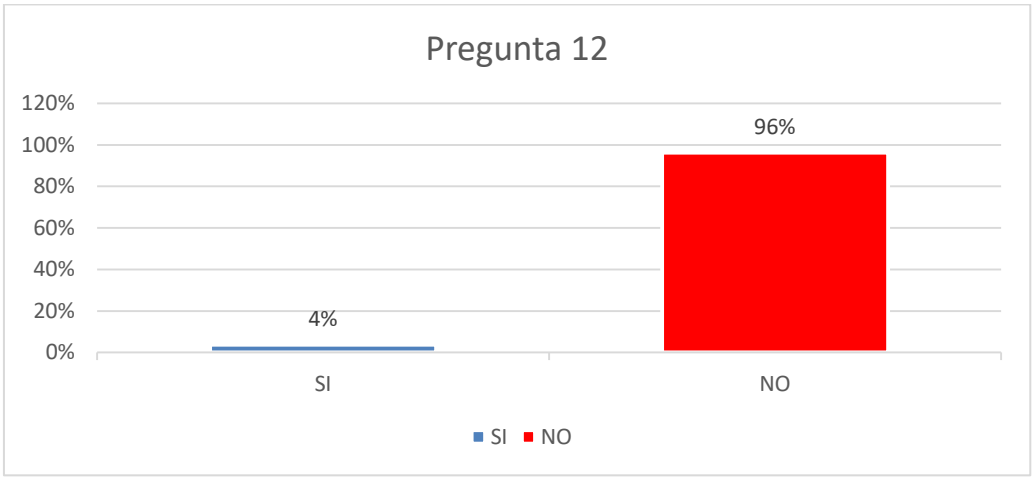
Tabla XII.

P12 ¿Cree usted que las fiscalías están preparadas para investigar delitos informáticos co eficacia?		
	Frecuencia	Porcentaje

SI	3	4%
NO	77	96%
Total	80	100%

Fuente: Data de resultados

Figura 12



Interpretación: En la Tabla XII, Figura 12, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión capacidad, donde apenas el 4% de los encuestados considera que las fiscalías están preparadas para investigar los delitos informáticos con eficacia, mientras que el 96% manifiesta que no cuentan con la preparación necesaria. Estos datos permiten identificar una percepción ampliamente negativa sobre la capacidad operativa y técnica de las fiscalías para enfrentar el cibercrimen. Resulta relevante destacar que esta insuficiente preparación no solo limita la investigación adecuada de los delitos informáticos, sino que también dificulta la identificación de los responsables y la obtención de pruebas digitales, afectando la eficacia del sistema de justicia penal. Asimismo, esta situación compromete derechos fundamentales como la seguridad jurídica, la tutela jurisdiccional efectiva y la protección de las víctimas, evidenciando la necesidad urgente de fortalecer las capacidades tecnológicas, la especialización del personal fiscal y los recursos institucionales en el contexto de la criminalidad digital.

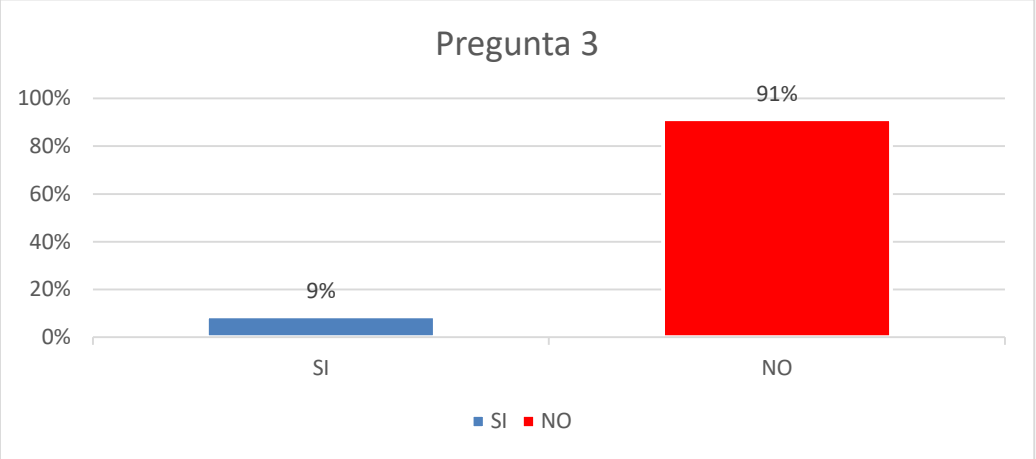
Tabla XIII.

P13 ¿Considera que la Policía Nacional cuenta con personal capacitado en delitos informáticos?		
	Frecuencia	Porcentaje

SI	7	9%
NO	73	91%
Total	80	100%

Fuente: Data de resultados

Figura 13



Interpretación: En la Tabla XIII, Figura 13, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión capacidad, donde solo el 9% de los encuestados considera que la Policía Nacional cuenta con personal capacitado para enfrentar los delitos informáticos, mientras que el 91% manifiesta que no existe una preparación adecuada en esta materia. Estos datos permiten identificar una percepción mayoritaria de insuficiente capacitación del personal policial frente a los desafíos que plantea la criminalidad digital. Resulta relevante destacar que la falta de personal especializado no solo dificulta la prevención, investigación y persecución de los delitos informáticos, sino que también limita la respuesta oportuna y eficaz ante este tipo de conductas ilícitas. Asimismo, esta carencia de capacitación compromete la protección de derechos fundamentales como la seguridad ciudadana, la integridad patrimonial y el acceso a una tutela efectiva, evidenciando la necesidad de fortalecer la formación especializada y los recursos humanos de la Policía Nacional en el ámbito de los delitos informáticos.

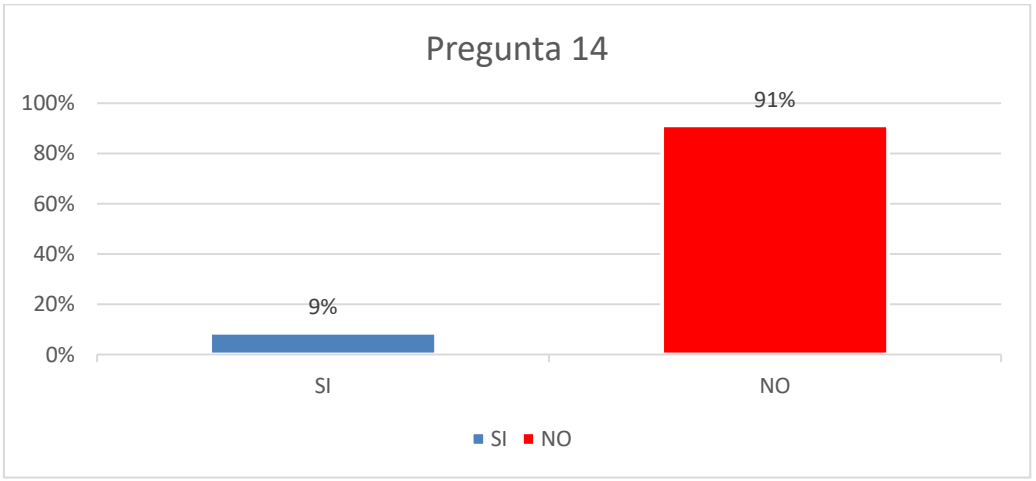
Tabla XIV.

P14 ¿Cree que los operadores de justicia reciben formación constante sobre criminalidad digital?

	Frecuencia	Porcentaje
SI	7	9%
NO	73	91%
Total	80	100%

Fuente: Data de resultados

Figura 14



Interpretación: En la Tabla XIV, Figura 14, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión capacidad, donde únicamente el 9% de los encuestados considera que los operadores de justicia reciben formación constante sobre criminalidad digital, mientras que el 91% manifiesta que dicha capacitación no se realiza de manera continua. Estos datos permiten identificar una percepción mayoritaria de insuficiencia en la formación especializada de los operadores de justicia frente a los retos que impone la criminalidad digital. Resulta relevante destacar que la falta de capacitación permanente no solo limita la correcta interpretación y aplicación de las normas penales en materia de delitos informáticos, sino que también afecta la eficacia de los procesos de investigación y juzgamiento. Asimismo, esta carencia formativa compromete derechos fundamentales como la tutela jurisdiccional efectiva, la seguridad jurídica y la protección de las víctimas, evidenciando la necesidad de implementar programas de capacitación continua y especializada en criminalidad digital dentro del sistema de justicia.

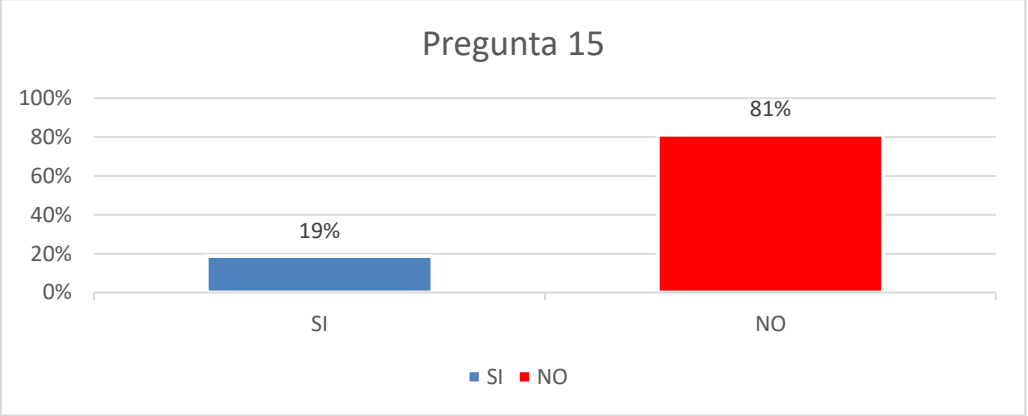
Tabla XV.

P15 ¿Considera que las víctimas de delitos informáticos reciben una respuesta oportuna po parte de las autoridades?

	Frecuencia	Porcentaje
SI	15	19%
NO	65	81%
Total	80	100%

Fuente: Data de resultados

Figura 15



Interpretación: En la Tabla XV, Figura 15, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión capacidad, donde únicamente el 19% de los encuestados considera que las víctimas de delitos informáticos reciben una respuesta oportuna por parte de las autoridades, mientras que el 81% manifiesta que dicha respuesta no es adecuada ni oportuna. Estos datos permiten identificar una percepción mayoritaria de ineficiencia en la atención que brindan las autoridades a las víctimas de delitos informáticos. Resulta relevante destacar que la falta de una respuesta oportuna no solo afecta la confianza ciudadana en el sistema de justicia, sino que también vulnera derechos fundamentales como la tutela jurisdiccional efectiva, la seguridad jurídica y el acceso a la justicia. Asimismo, esta situación evidencia la necesidad de fortalecer los mecanismos de atención, orientación y acompañamiento a las víctimas, así como de mejorar la capacidad de respuesta institucional frente a la criminalidad digital.

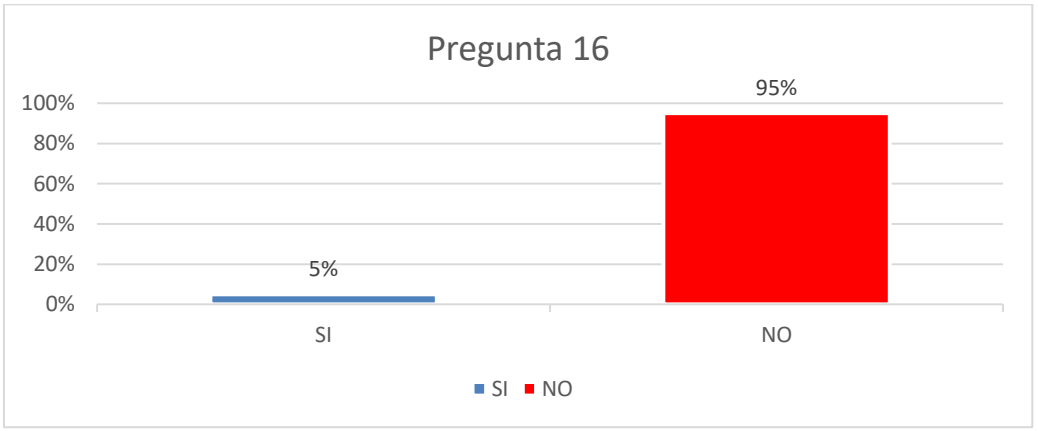
Dimensión: eficacia

Tabla XVI.

P16 ¿Considera que las normas penales vigentes en el Perú son eficaces para sancionar los delitos informáticos?		
	Frecuencia	Porcentaje
SI	4	5%
NO	76	95%
Total	80	100%

Fuente: Data de resultados

Figura 16



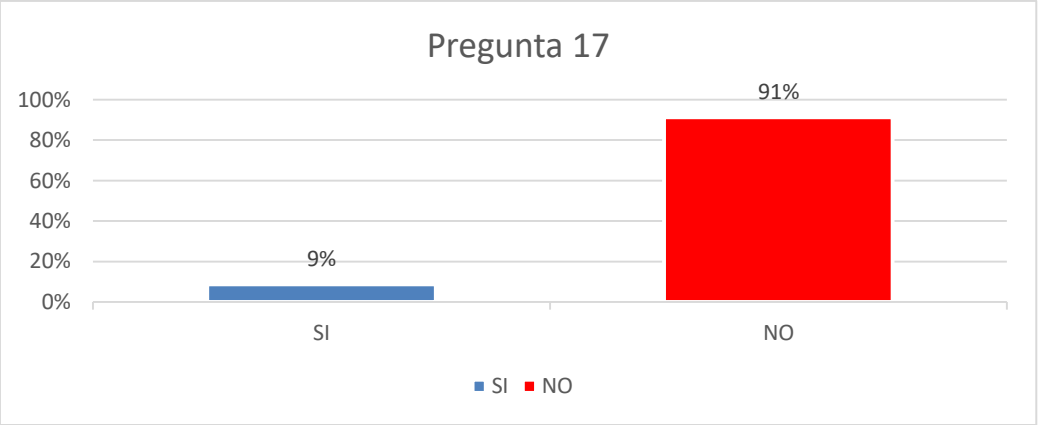
Interpretación: En la Tabla XVI, Figura 16, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión eficacia, donde solo el 5% de los encuestados considera que las normas penales vigentes en el Perú son eficaces para sancionar los delitos informáticos, mientras que el 95% manifiesta que dichas normas no resultan eficaces. Estos datos permiten identificar una percepción ampliamente negativa respecto a la eficacia del marco normativo penal frente a los delitos informáticos. Resulta relevante destacar que la insuficiencia de normas eficaces no solo dificulta la adecuada sanción de estas conductas ilícitas, sino que también limita su efecto disuasivo, favoreciendo la reiteración de los delitos en el entorno digital. Asimismo, esta situación compromete derechos fundamentales como la seguridad jurídica, la tutela jurisdiccional efectiva y la protección de las víctimas, evidenciando la necesidad de actualizar, fortalecer y adecuar la legislación penal a las nuevas modalidades delictivas propias de la era digital.

Tabla XVII.

P17 ¿Cree usted que la legislación penal actual está actualizada frente a las nuevas modalidades

de delitos informáticos?		
	Frecuencia	Porcentaje
SI	7	9%
NO	73	91%
Total	80	100 %

Figura 17



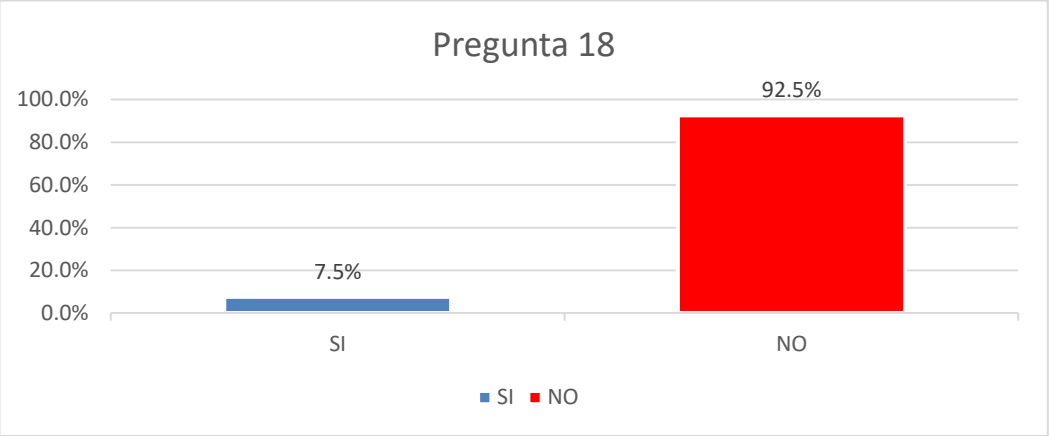
Interpretación: En la Tabla XVII, Figura 17, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión eficacia, donde solo el 9% de los encuestados considera que la legislación penal actual se encuentra actualizada frente a las nuevas modalidades de delitos informáticos, mientras que el 91% manifiesta que dicha normativa no responde adecuadamente a las exigencias del contexto digital. Estos datos permiten identificar una percepción mayoritaria de desactualización del marco legal penal frente a la evolución constante de la criminalidad informática. Resulta relevante destacar que la falta de actualización normativa no solo limita la correcta tipificación y sanción de nuevas conductas delictivas, sino que también reduce la capacidad preventiva del derecho penal. Asimismo, esta situación afecta derechos fundamentales como la seguridad jurídica y la tutela jurisdiccional efectiva, evidenciando la necesidad de una revisión y modernización permanente de la legislación penal para enfrentar de manera eficaz los desafíos propios de la era digital.

Tabla XVIII.

P18 ¿Piensa que existen vacíos legales que dificultan la sanción de los delitos informáticos?		
	Frecuencia	Porcentaje
SI	6	7.5%
NO	74	92.5%
Total	80	100%

Fuente: Data de resultados

Figura 18



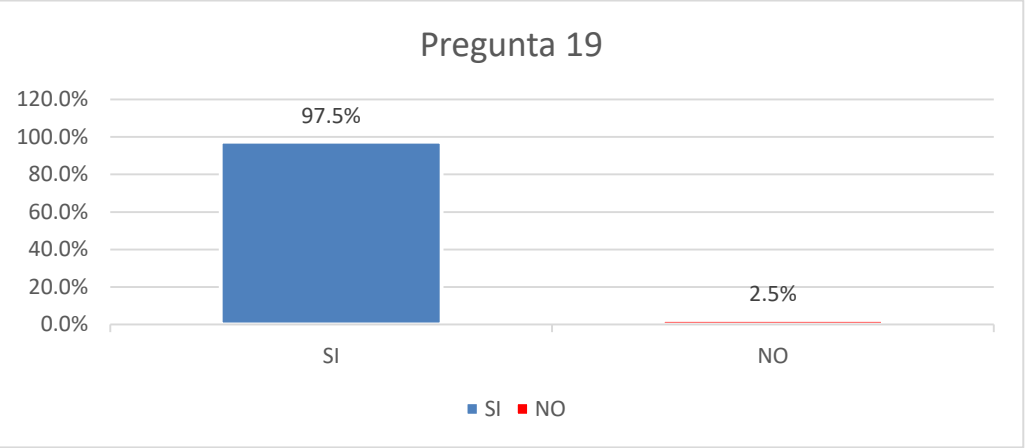
Interpretación: En la Tabla XVIII, Figura 18, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión eficacia, donde el 7,5% de los encuestados considera que existen vacíos legales que dificultan la sanción de los delitos informáticos, mientras que el 92,5% manifiesta que no percibe la existencia de dichos vacíos. Estos datos permiten identificar que, desde la percepción mayoritaria de los participantes, el marco normativo penal contaría con disposiciones suficientes para la sanción de los delitos informáticos. Resulta relevante destacar que esta apreciación sugiere una confianza relativa en la estructura legal vigente; sin embargo, el reducido porcentaje que sí identifica vacíos legales evidencia que aún existen cuestionamientos sobre la claridad, precisión o adecuación de algunas normas frente a determinadas modalidades delictivas. Asimismo, esta situación pone de manifiesto la importancia de evaluar de manera continua la eficacia real de la legislación penal, a fin de garantizar la correcta protección de derechos fundamentales como la seguridad jurídica, la tutela jurisdiccional efectiva y la adecuada sanción de las conductas ilícitas en el entorno digital.

Tabla XIX.

P19 ¿Considera que el Código Penal peruano requiere reformas urgentes en materia de criminalidad informática?		
	Frecuencia	Porcentaje
SI	78	97.5%
NO	2	2.5%
Total	80	100%

Fuente: Data de resultados

Figura 19



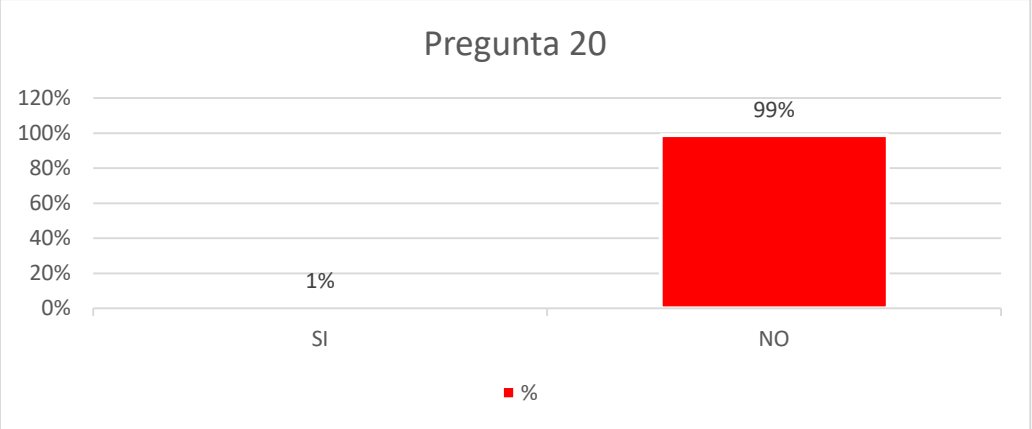
Interpretación: En la Tabla XIX, Figura 19, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión eficacia, donde el 97,5% de los encuestados considera que el Código Penal peruano requiere reformas urgentes en materia de criminalidad informática, mientras que solo el 2,5% manifiesta una opinión contraria. Estos datos permiten identificar una percepción ampliamente mayoritaria sobre la necesidad de actualizar y reformar el marco penal vigente frente a los desafíos que plantea la criminalidad digital. Resulta relevante destacar que esta demanda de reformas urgentes refleja la insuficiencia del Código Penal actual para responder de manera eficaz a las nuevas modalidades de delitos informáticos, lo que limita su capacidad preventiva y sancionadora. Asimismo, la falta de adecuación normativa compromete la protección de derechos fundamentales como la seguridad jurídica, la tutela jurisdiccional efectiva y la protección de las víctimas, evidenciando la urgencia de una reforma integral que fortalezca la regulación penal en la era digital.

Tabla XX.

P20 ¿Cree usted que la normativa penal contempla adecuadamente la responsabilidad penal de los menores en delitos informáticos?		
	Frecuencia	Porcentaje
SI	1	1%
NO	79	99%
Total	80	100%

Fuente: Data de resultados

Figura 20



Interpretación: En la Tabla XX, Figura 20, se presentan las respuestas de los 80 participantes respecto a la variable regulación penal en la era digital, en la dimensión eficacia, donde solo el 1% de los encuestados considera que la normativa penal contempla adecuadamente la responsabilidad penal de los menores en delitos informáticos, mientras que el 99% manifiesta que dicha regulación resulta insuficiente. Estos datos permiten identificar una percepción casi unánime sobre la inadecuada regulación de la responsabilidad penal de los menores frente a los delitos informáticos. Resulta relevante destacar que esta carencia normativa no solo dificulta el tratamiento jurídico adecuado de estas conductas, sino que también limita la aplicación de medidas diferenciadas orientadas a la prevención, rehabilitación y sanción proporcional. Asimismo, la falta de una regulación específica y eficaz compromete la protección de derechos fundamentales como el interés superior del niño y adolescente, la seguridad jurídica y la tutela efectiva, evidenciando la necesidad de incorporar disposiciones claras y actualizadas que respondan a la participación de menores en la criminalidad digital.

Prueba de normalidad

H_0: Los datos tienen distribución normal

p > 0,05

H_1: Los datos no tienen distribución normal

Nivel de significancia: $\alpha = 0.05$

Tabla XXI.

Prueba de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DELITOS INFORMATICOS	0.123	80	0.004	0.945	80	0.002
REGULACIÓN PENAL EN LA ERA DIGITAL	0.205	80	0.000	0.887	80	0.000

a. Corrección de significación de Lilliefors

Fuente: Data de resultados

Los resultados de las pruebas de normalidad Kolmogorov-Smirnov evidenciaron que ambas variables, Delitos informáticos y regulación penal en la era digital, presentan valores de significancia inferiores al nivel crítico establecido ($p < 0.05$). En consecuencia, se rechaza la hipótesis nula que asume una distribución normal de los datos y se confirma que ambas variables no siguen una distribución normal. Debido a ello, se optó por emplear un método no paramétrico para el análisis correlacional, utilizando el coeficiente Rho de Spearman, adecuado para datos que no cumplen con el supuesto de normalidad.

Prueba de hipótesis general

Hipótesis nula: Ho: $r_{xy} = 0$

Los delitos informáticos no constituyen un desafío creciente para la regulación penal en el Distrito Fiscal de Ica, debido a su constante evolución tecnológica y limitada adaptación normativa, en el año 2024.

Hipótesis alterna: Ha: $\rho\ r_{xy} \neq 0$

Los delitos informáticos constituyen un desafío creciente para la regulación penal en el Distrito Fiscal de Ica, debido a su constante evolución tecnológica y limitada adaptación normativa, en el año 2024.

Nivel de significación:

α = 0.05 (prueba bilateral)

Regla de decisión:

p > α = acepta H_0 se rechaza la hipótesis alterna

$p < \alpha$ = rechaza H_0 se acepta la hipótesis alterna

Estadígrafo de Prueba:

Coeficiente de correlación de Rho de Spearman

			VARX: DELITOS INFORMATICOS	VARY: REGULACIÓN PENAL EN LA ERA DIGITAL
Rho de Spearman	VARX: DELITOS INFORMATICOS	Coeficiente de correlación	1.000	0,379**
		Sig. (bilateral)		0.001
		N	80	80
	VARY: REGULACIÓN PENAL EN LA ERA DIGITAL	Coeficiente de correlación	0,379**	1.000
		Sig. (bilateral)	0.001	
		N	80	80

De acuerdo con la prueba de correlación de Rho de Spearman, se obtuvo un coeficiente de correlación de $r_s = 0.379$ con un valor de $p = 0.001$, el cual es menor que el nivel de significancia establecido ($\alpha = 0.05$). En consecuencia, se rechaza la hipótesis nula y se acepta la hipótesis alterna, concluyéndose que existe una relación estadísticamente relevante entre los delitos informáticos y regulación penal en la era digital en el distrito fiscal de Ica, año 2024. Por lo que, se puede afirmar que los delitos informáticos si constituyen un desafío creciente para la regulación penal en el Distrito Fiscal de Ica, debido a su constante evolución tecnológica y limitada adaptación normativa, en el año 2024. En consecuencia, existe correlación entre las variables de estudio, mostrando una relación consistente desde el punto de vista estadístico.

Prueba de hipótesis específica 1

Hipótesis nula: Ho: $r_{xy} = 0$

El incremento del delito de phishing no influye negativamente en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024.

Hipótesis alterna: Ha: $\rho\ r_{xy} \neq 0$

El incremento del delito de phishing influye negativamente en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024.

Nivel de significación:

α = 0.05 (prueba bilateral)

Regla de decisión:

$p > \alpha$ = acepta H_0 se rechaza la hipótesis alterna

$p < \alpha$ = rechaza H_0 se acepta la hipótesis alterna

Estadígrafo de Prueba:

Coeficiente de Correlación de Rho de Spearman.

			D1: PHISHING	D1: CAPACIDAD
Rho de Spearman	D1: PHISHING	Coeficiente de correlación	1.000	0.379
		Sig. (bilateral)		0.001
		N	80	80
	D1: CAPACIDAD	Coeficiente de correlación	0.379	1.000
		Sig. (bilateral)	0.001	
		N	80	80

De acuerdo con la prueba de correlación de Rho de Spearman, se obtuvo un coeficiente de correlación de $r_s = 0.379$ y un valor de $p = 0.001$, el cual es menor que el nivel de significancia establecido ($\alpha = 0.05$). En consecuencia, se rechaza la hipótesis nula y se acepta la hipótesis alterna, determinándose que existe una relación estadísticamente significativa entre el delito de Phishing y la capacidad del sistema penal en el distrito fiscal de Ica, año 2024. Por tanto, se puede afirmar que el incremento del delito de phishing influye negativamente en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024; esta relación es estadísticamente significativa, lo que confirma la existencia de un vínculo real entre ambas variables.

Prueba Hipótesis específica 2

Hipótesis nula: Ho: $r_{xy} = 0$

La continua incidencia del fraude informático no evidencia las limitaciones del marco normativo penal, reduciendo su eficacia frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024.

Hipótesis alterna: Ha: $\rho\ r_{xy} \neq 0$

La continua incidencia del fraude informático evidencia las limitaciones del marco normativo penal, reduciendo su eficacia frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024.

Nivel de significación:

α = 0.05 (prueba bilateral)

Regla de decisión:

$p > \alpha$ = acepta H_0 se rechaza la hipótesis alterna

$p < \alpha$ = rechaza H_0 se acepta la hipótesis alterna

Estadígrafo de Prueba:

Coeficiente de Correlación de Rho de Spearman

			D2: FRAUDE INFORMATICO	D2: EFICACIA
Rho de Spearman	D2: FRAUDE INFORMATICO	Coeficiente de correlación	1.000	0,238*
		Sig. (bilateral)		0.033
		N	80	80
	D2: EFICACIA	Coeficiente de correlación	0,238*	1.000
		Sig. (bilateral)	0.033	
		N	80	80

De acuerdo con la prueba de correlación de Rho de Spearman, se obtuvo un coeficiente de correlación de $r_s = 0.238$ y un valor de $p = 0.033$, el cual es menor que el nivel de significancia establecido ($\alpha = 0.05$). En consecuencia, se rechaza la hipótesis nula y se acepta la hipótesis alterna, concluyéndose que sí existe una relación estadísticamente importante entre el delito de fraude informático y la eficacia de la regulación penal en el distrito fiscal de Ica, año 2024. El coeficiente positivo indica que, la continua incidencia del fraude informático evidencia las limitaciones del marco normativo penal, reduciendo su eficacia frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024; esta relación es estadísticamente significativa, lo que confirma la existencia de un vínculo real entre ambas variables.

IV. DISCUSIÓN DE RESULTADOS

En esta sección de la Tesis se realizó la discusión de las hipótesis específicas, posteriormente, de la hipótesis general; para lo cual se tomaron en cuenta los resultados plasmados en las correspondientes Tablas, Figuras, asimismo, considerando algún antecedente o base teórica, por último, por cada discusión se ha consignado el aporte de la investigadora.

En la **Hipótesis Específica 1** se planteó que el incremento del delito de phishing influye negativamente en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024. Para contrastar, validar y confirmar esta hipótesis se recurre a los Resultados de la Tabla II, Figura 2, en donde, de la encuesta realizada a 80 participantes, se revela que un 89% de los encuestados manifiesta haber observado un aumento en las denuncias por phishing en los últimos años, mientras que el 11% indica no haber percibido dicho incremento. Asimismo, los Resultados de Tabla XV, Figura 15 nos muestran que de los 80 sujetos encuestados; 19% de los encuestados considera que las víctimas de delitos informáticos reciben una respuesta oportuna por parte de las autoridades, mientras que el 81% manifiesta que dicha respuesta no es adecuada ni oportuna. Lo expuesto, guarda concordancia con lo señalado por Akobari, et.al. (2024) quienes señalan que "el phishing y los engaños en el ámbito digital son técnicas cada vez más sofisticadas utilizadas por los ciberdelincuentes para obtener información confidencial de manera fraudulenta"

Ello evidencia que el incremento sostenido del delito de phishing no solo afecta directamente a las víctimas, sino que también desborda la capacidad operativa y de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica. La alta incidencia de denuncias, sumada a la complejidad técnica de estos delitos y a la constante evolución de las modalidades delictivas digitales, genera retrasos en la investigación, dificultades en la identificación de los responsables y una percepción generalizada de ineficacia institucional. Esta situación propicia un escenario de desconfianza ciudadana, en el cual las víctimas perciben que sus denuncias no reciben una atención adecuada ni oportuna, debilitando así la función preventiva y sancionadora del sistema penal y favoreciendo la continuidad de estas conductas ilícitas.

En tal sentido, se considera que el fortalecimiento de la capacidad de respuesta del sistema penal resulta imprescindible para enfrentar eficazmente el delito de phishing. Ello implica la implementación de políticas públicas orientadas a la especialización y capacitación constante de fiscales, policías y personal técnico en materia de delitos informáticos, así como la dotación de recursos tecnológicos adecuados para la investigación digital. Asimismo, la articulación interinstitucional y la promoción de mecanismos de atención rápida y especializada a las

víctimas permitirían mejorar la eficacia de las investigaciones y la percepción de justicia. De esta manera, se contribuiría a una respuesta penal más eficiente, disuasiva y acorde con la dinámica actual de la criminalidad informática, fortaleciendo la confianza ciudadana y la protección de los derechos en el entorno digital.

En la **Hipótesis Específica 2** se formuló que la continua incidencia del fraude informático evidencia las limitaciones del marco normativo penal, reduciendo su eficacia frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024. Para confirmar dicha hipótesis recurriremos a la Tabla VI, Figura 6, donde de las 80 personas encuestadas el 84% de los encuestados considera que el fraude informático se ha convertido en uno de los delitos más comunes en el ámbito digital, mientras que el 16% manifiesta no compartir dicha percepción. Asimismo; resulta pertinente remitirnos a la Tabla XVII, Figura 17, donde de las 80 personas que conforman la muestra representativa, donde solo el 9% de los encuestados considera que la legislación penal actual se encuentra actualizada frente a las nuevas modalidades de delitos informáticos, mientras que el 91% manifiesta que dicha normativa no responde adecuadamente a las exigencias del contexto digital. Lo señalado encuentra concordancia con Bravo (2024), quien señala "En los últimos años, el fraude informático ha aumentado considerablemente, convirtiéndose en una de las principales amenazas para la economía y la seguridad digital en el Perú. Este crecimiento está ligado al uso masivo de internet y plataformas digitales, que han transformado las dinámicas comerciales, sociales y financieras".

Ello evidencia que la continua incidencia del fraude informático no solo refleja el incremento de conductas delictivas en el entorno digital, sino que pone de manifiesto las limitaciones estructurales y normativas del marco penal vigente para hacerles frente de manera eficaz en el Distrito Fiscal de Ica. La percepción mayoritaria de los encuestados respecto a la falta de actualización de la legislación penal demuestra que las normas existentes no se encuentran plenamente alineadas con la dinámica cambiante de las nuevas modalidades de fraude informático, lo que dificulta su correcta tipificación, persecución y sanción. Esta brecha normativa genera vacíos legales que son aprovechados por los delincuentes, reduciendo el efecto disuasivo de la ley y debilitando la confianza de la ciudadanía en la capacidad del sistema penal para proteger sus derechos en el ámbito digital.

En tal sentido, se considera indispensable la revisión y actualización integral del marco normativo penal en materia de delitos informáticos, a fin de adecuarlo a las exigencias del contexto tecnológico actual. Ello debe ir acompañado de la incorporación de tipos penales específicos, el fortalecimiento de las herramientas jurídicas para la investigación digital y la capacitación especializada de los operadores de justicia. Asimismo, resulta necesario promover

una política criminal orientada a la prevención del fraude informático, mediante campañas de educación digital y mecanismos de cooperación interinstitucional. De esta manera, se contribuirá a mejorar la eficacia del sistema penal, fortalecer la seguridad jurídica y garantizar una respuesta oportuna y efectiva frente a los delitos informáticos, en beneficio de la protección de la sociedad y del desarrollo seguro del entorno digital.

Por último, en la **Hipótesis General** se esgrimió que los delitos informáticos constituyen un desafío creciente para la regulación penal en el Distrito Fiscal de Ica, debido a su constante evolución tecnológica y limitada adaptación normativa, en el año 2024. Para confirmar dicha hipótesis resulta pertinente recurrir a la Tabla XI, Figura 11; donde de las 80 personas encuestadas solo el 6% de los encuestados considera que el sistema penal cuenta con suficientes herramientas tecnológicas para enfrentar el cibercrimen, mientras que el 94% manifiesta que dichas herramientas resultan insuficientes. Asimismo, se tiene de la Tabla XVI, Figura 16; que de los 80 participantes solo el 5% de los encuestados considera que las normas penales vigentes en el Perú son eficaces para sancionar los delitos informáticos, mientras que el 95% manifiesta que dichas normas no resultan eficaces. Lo señalado guarda concordancia con lo señalado por Corrales (2024) quien en la concusión a la que arribó en su investigación, señaló que, en la era digital, los ciberdelitos o delitos informáticos presentan una serie de desafíos complejos que requieren un análisis profundo desde el derecho penal, tanto en su estructura básica como en su aplicación pura.

Este escenario evidencia que los delitos informáticos constituyen un desafío estructural y creciente para la regulación penal en el Distrito Fiscal de Ica, en la medida en que la acelerada evolución tecnológica ha superado ampliamente la capacidad de adaptación del sistema penal vigente. La percepción mayoritaria de los encuestados respecto a la insuficiencia de herramientas tecnológicas y a la ineficacia de las normas penales refleja una brecha significativa entre la realidad del cibercrimen y los mecanismos institucionales destinados a enfrentarlo. Esta situación limita la capacidad del Estado para investigar, perseguir y sancionar adecuadamente estas conductas, debilitando la función preventiva del derecho penal y generando una sensación de impunidad que favorece la expansión de los delitos informáticos en el entorno digital.

En tal sentido, resulta imprescindible el fortalecimiento integral del sistema penal frente al cibercrimen, lo cual exige no solo la actualización y especialización del marco normativo, sino también la implementación de herramientas tecnológicas modernas y la capacitación permanente de los operadores de justicia. Asimismo, se hace necesaria la adopción de una política criminal coherente con las dinámicas digitales, que promueva la cooperación interinstitucional y el intercambio de información especializada, tanto a nivel nacional como

internacional. De esta manera, se contribuirá a consolidar una respuesta penal más eficaz, oportuna y acorde con las exigencias de la era digital, garantizando una mayor protección jurídica y fortaleciendo la confianza ciudadana en el sistema de justicia penal en el Distrito Fiscal de Ica.

V. CONCLUSIONES

1) Luego del análisis de la información obtenida en las dimensiones “phishing” y “capacidad”, a partir de los instrumentos de recolección aplicados, se concluye que —tal como se observa en la Tabla II (Figura 2) y en la Tabla XV (Figura 15)— el incremento sostenido del delito de phishing constituye un factor que afecta negativamente la capacidad de respuesta del sistema penal frente a los delitos informáticos. En efecto, ello se evidencia en la medida en que el notable aumento de las denuncias por phishing no ha sido acompañado por una respuesta institucional oportuna y eficaz por parte de las autoridades competentes. Esta situación limita la atención adecuada a las víctimas, debilita la eficacia del sistema penal y favorece una percepción de ineficiencia e impunidad, comprometiendo la capacidad del Estado para enfrentar de manera efectiva el cibercrimen en el Distrito Fiscal de Ica durante el año 2024.

2) Del análisis de la información obtenida en las dimensiones “fraude informático” y “eficacia”, a partir de los instrumentos de recolección aplicados, se concluye que —tal como se observa en la Tabla VI (Figura 6) y en la Tabla XVII (Figura 17)— la alta incidencia del fraude informático constituye un factor que afecta negativamente la eficacia del marco normativo penal frente a los delitos informáticos. En efecto, ello se evidencia en la medida en que la creciente frecuencia de este tipo de conductas delictivas en el ámbito digital no ha sido acompañada por una adecuada actualización de la legislación penal, lo que limita su capacidad de respuesta frente a las nuevas modalidades delictivas. Esta situación genera vacíos normativos y reduce el efecto disuasivo de la norma penal, comprometiendo la eficacia del sistema de justicia y dificultando la persecución y sanción efectiva del fraude informático en el Distrito Fiscal de Ica durante el año 2024.

3) Luego del análisis de la información obtenida en las variables “delitos informáticos” y “regulación penal en la era digital”, a partir de los instrumentos de recolección aplicados, se concluye que —tal como se observa en la Tabla XI (Figura 11) y en la Tabla XVI (Figura 16)— los delitos informáticos constituyen un verdadero desafío con relación a la eficacia de la regulación penal en la era digital. En efecto, ello se evidencia en la medida en que la insuficiencia de herramientas tecnológicas y la limitada eficacia de las normas penales vigentes restringen la capacidad del sistema penal para enfrentar adecuadamente el cibercrimen. Esta situación debilita los mecanismos de prevención, investigación y sanción de los delitos informáticos, generando una respuesta institucional deficiente y una percepción de impunidad, lo cual compromete la protección de los derechos digitales y la efectividad del sistema de justicia penal en el Distrito Fiscal de Ica durante el año 2024.

VI. RECOMENDACIONES

1) Se recomienda fortalecer de manera prioritaria las unidades especializadas en delitos informáticos dentro del Distrito Fiscal de Ica, mediante la capacitación continua de fiscales, personal policial y peritos en investigación digital. Asimismo, resulta necesario dotar a estas instancias de herramientas tecnológicas adecuadas que permitan una atención oportuna y eficaz de las denuncias, con el fin de reducir los tiempos de respuesta, mejorar la atención a las víctimas y fortalecer la confianza ciudadana en el sistema de justicia frente a este tipo de delitos.

2) Se recomienda impulsar una revisión y actualización integral de la legislación penal vigente en materia de delitos informáticos, incorporando tipos penales específicos que respondan a las nuevas modalidades de fraude informático. Esta actualización normativa debe ir acompañada de criterios claros de aplicación y sanción, a fin de cerrar vacíos legales, fortalecer el efecto disuasivo de la norma penal y garantizar una persecución más efectiva de estas conductas ilícitas en el entorno digital.

3) Se recomienda diseñar e implementar una política criminal integral orientada al cibercrimen, que articule la modernización normativa, el fortalecimiento tecnológico y la cooperación interinstitucional, tanto a nivel nacional como internacional. Asimismo, se sugiere promover programas de prevención y educación digital dirigidos a la ciudadanía, con el propósito de reducir la vulnerabilidad frente a los delitos informáticos y consolidar un sistema penal más eficaz, moderno y acorde con las exigencias del contexto digital en el Distrito Fiscal de Ica.

VII. REFERENCIAS BIBLIOGRÁFICAS

Aguirre, R., & Jiménez, C. (2020). Tecnologías de la información y la comunicación para la conservación y promoción de la diversidad cultural en el marco del pluralismo jurídico. Revista Digital de Derecho Administrativo, (22), 1–15.

Akbari, Y., Al Maadeed, S., Elharrouss, O., Ottakath, N., & Khelifi, F. (2024). Hierarchical deep learning approach using fusion layer for source camera model identification based on video taken by smartphone. Expert Systems with Applications, 238, 1–10. https://doi.org/10.1016/j.eswa.2023.121603

Alcántara Díaz, F. E. (2024). Análisis de la Ley N.° 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022 [Tesis de posgrado]. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/12384

Añasco, C., Morocho, K., & Hallo, M. (2023). Using data mining techniques for the detection of SQL injection attacks on database systems. Revista Politécnica, 51(2), 19–28. https://doi.org/10.33333/rp.vol51n2.02

Arias, L. A. (2021). Limitaciones del sistema penal para investigar y probar la comisión del ciberdelito en El Salvador [Tesis de posgrado]. Universidad de El Salvador. https://ri.ues.edu.sv/id/eprint/26913/

Besares, A. (2015). Tópicos de derecho informático. UNACH. https://www.iijunach.mx/images/publicaciones/Topicos_de_Derecho_Informatico.pdf

Bravo Acosta, G. (2024). Necesidad de la variación del marco punitivo establecido en el delito de fraude informático en la legislación peruana [Tesis de posgrado]. Universidad Tecnológica del Perú. https://repositorio.utp.edu.pe/handle/20.500.12867/11819

Colorado Aguirre, R. R. (2025). Delitos cibernéticos y la protección de datos personales en la era digital. Polo del Conocimiento. https://polodelconocimiento.com/ojs/index.php/es/article/view/9818

Díaz Basurto, I. J., Ojeda Sotomayor, P. M., Cajas Parraga, C. M., & Cabrera Ripalda, E. P. (2023). Desafíos legales en Ecuador frente a los delitos informáticos: Importancia de su prevención. Universidad y Sociedad, 15(6), 746–754. https://rus.ucf.edu.cu/index.php/rus/article/view/4195

Fernández Altamirano, A. (2024). El derecho penal y procesal penal en la era digital: desafíos y oportunidades. Universidad César Vallejo. https://www.ucv.edu.pe/noticias/el-derecho-penal-y-procesal-penal-en-la-era-digital-desafios-y-oportunidades

Flores, L. L. (2014). Derecho informático. Patria.

Fu, B., Wang, Y., & Feng, T. (2024). CT-GCN+: A high-performance cryptocurrency transaction graph convolutional model for phishing node classification. Cybersecurity, 7(3), 1–16. https://doi.org/10.1186/s42400-023-00194-5

Hamdi, K., Padilla, J. J., Vernon-Bido, D., Saikou, Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. Journal of Cybersecurity, 7(1), 1–13. https://doi.org/10.1093/cybsec/tyab005

Macías-Lara, R. A., Boné Andrade, M. F., Quiñonez Angulo, F., Mendoza Loor, J. J., Estupiñán-Troya, G., & Rodríguez Vizuete, J. D. (2022). Frequent cases, criminalization and prevention of computer crimes in Ecuador: A brief systematic review. Sapienza: International Journal of Interdisciplinary Studies, 3(2), 231–243. https://doi.org/10.51798/sijis.v3i2.324

Muñoz Sánchez, M. A. (2024). Acceso a la cultura judicial del derecho penal y regulación de los delitos informáticos en el Distrito Judicial de Pasco, 2021 [Tesis de posgrado]. Universidad Nacional Daniel Alcides Carrión. http://45.177.23.200/handle/undac/4768

Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 [Tesis de posgrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/20372

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

Rivera de la Cruz, A. (2025). El papel del Estado en la lucha contra los delitos informáticos en el Perú [Tesis de posgrado]. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/14504

Rodríguez Vega, P. E. (2023). Importancia jurídica social de la implementación en la calificación y tipificación de los delitos informáticos en la provincia de Ica [Tesis de pregrado]. Universidad Nacional San Luis Gonzaga. https://repositorio.unica.edu.pe/items/2d27e812-b1a2-43cf-a2da-c3e64cc222de

Rojas López, E. (2024). La necesidad de regulación de nuevas modalidades del delito de fraude informático frente a la ciberdelincuencia en el Perú, 2023 [Tesis de posgrado]. Universidad Privada del Norte. https://repositorio.upn.edu.pe/handle/11537/41216

Rosales Medina, R. M. (2024). Incremento de los delitos informáticos y su problemática con la impunidad delictiva en Lima, 2024 [Tesis de posgrado]. Universidad Autónoma del Perú. https://repositorio.autonoma.edu.pe/handle/20.500.13067/3793

Roztocki, N., Soja, P., & Weistroffer, H. R. (2019). The role of information and communication technologies in socioeconomic development: Towards a multidimensional framework. Information Technology for Development, 25(2), 171–183. https://doi.org/10.1080/02681102.2019.1596654

Sánchez, F. (2019). Guía de tesis y proyectos de investigación. Centrum Legalis E.I.R.L.

Tavares, A., & Bitencourt, C. (2021). Diálogo entre o direito e a engenharia de software para um novo paradigma de transparência: Controle social digital. Revista Eurolatinoamericana de Derecho Administrativo, 8(1), 9–34. https://doi.org/10.14409/redoeda.v8i1.9676

Van Dijk, J., & Van Deursen, A. (2014). Digital skills: Unlocking the information society. Palgrave Macmillan.

Villavicencio Terreros, F. A. (2014). Delitos informáticos. Grijley.

VIII. ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA

ANEXO 2: MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

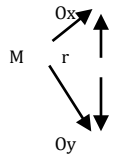
ANEXO 3: INSTRUMENTOS DE RECOLECCIÓN DE DATOS

ANEXO 4: DATA DE RESULTADOS

ANEXO 5: INFOGRAFIAS Y ESQUEMAS ALUSIVOS AL TEMA INVESTIGADO

ANEXO 6: ESCALA DE VALIDACIÓN DEL JEUZ EXPERTO

MATRIZ DE CONSISTENCIA DE LA TESIS

MATRIZ DE CONSISTENCIA DE LA TESIS "LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024"						
PROBLEMAS	**OBJETIVOS**	**HIPOTESIS**	**VARIABLES**	**INDICADORES**	**TECNICAS/ INSTRUMENTOS**	**METODOLOGÍA.**
GENERAL ¿De qué manera los delitos informáticos suponen un desafío para la regulación penal en el Distrito Fiscal de Ica, año 2024? **PROBLEMA ESPECÍFICO 1**. ¿Cómo influye el incremento del delito de phishing en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024? **PROBLEMA ESPECÍFICO 2** ¿Qué impacto tiene la incidencia del fraude informático en las limitaciones del marco normativo penal en el Distrito Fiscal de Ica, año 2024?	**GENERAL.** Analizar de qué manera los delitos informáticos suponen un desafío para la regulación penal en el Distrito Fiscal de Ica, año 2024. **OBJETIVO ESPECÍFICO 1:** Establecer cómo el incremento del delito de phishing influye en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024. **OBJETIVO ESPECÍFICO 2:** Determinar el impacto de la incidencia del fraude informático en las limitaciones del marco normativo penal en el Distrito Fiscal de Ica, año 2024.	**GENERAL** Los delitos informáticos constituyen un desafío creciente para la regulación penal en el Distrito Fiscal de Ica, debido a su constante evolución tecnológica y limitada adaptación normativa, en el año 2024. **HIPÒTESIS ESPECÌFICA 1:** El incremento del delito de phishing influye negativamente en la capacidad de respuesta del sistema penal frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024. **HIPÒTESIS ESPECÌFICA 2:** La continua incidencia del fraude informático evidencia las limitaciones del marco normativo penal, reduciendo su eficacia frente a los delitos informáticos en el Distrito Fiscal de Ica, año 2024.	**Variable X** DELITOS INFORMÁTICOS **DIMENSIONES** PHISHING FRAUDE INFORMÁTICO **Variable Y** REGULACIÓN PENAL EN LA ERA DIGITAL **DIMENSIONES** CAPACIDAD EFICACIA	**DE LA VARIABLE X:** INCREMENTO DE PHISHING COMO DELITO INFORMÁTICO FRECUENCIA DEL FRAUDE INFORMÁTICO COMO DELITO INFORMÁTICO **DE LA VARIABLE Y:** CAPACIDAD DE RESPUESTA DEL SISTEMA PENAL EFICACIA NORMATIVA	**TECNICA:** Encuesta **INSTRUMENTO:** CUESTIONARIO SOBRE DELITOS INFORMÁTICOS **TECNICA:** Encuesta **INSTRUMENTO:** CUESTIONARIO SOBRE REGULACIÓN PENAL EN LA ERA DIGITAL	**ENFOQUE: CUANTITATIVO.** Este enfoque permite sistematizar la información mediante cuadros estadísticos que reflejan la frecuencia, tipología y tendencia de los delitos informáticos, así como los niveles de respuesta institucional ante ellos. **TIPO.** BASICO **NIVEL.** CORRELACIONAL **DISEÑO DE INVESTIGACIÓN:** Corresponde a una investigación DESCRIPTIVO -CORRELACIONAL que se representa:  En donde: **M:** Fiscales, jueces, abogados penalistas, policías de la DIVINCRI y público general. **Ox:** Delitos Informáticos **Oy:** Regulación penal en la era digital. **R:** Factor de correlación. **Población:** 100 individuos **Muestra:** Estará conformada por 80 personas. **Muestreo:** No Probabilístico.

MATRIZ DE OPERALIZACIÓN DE VARIABLES DE LA TESIS

“Los delitos informáticos y su regulación en el sistema penal: un análisis de los nuevos desafíos en la era digital del distrito fiscal de Ica, año 2024”

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES/ INDICADORES	ITEMS	ESCALA DE MEDICIÓN
VARIABLE X DELITOS INFORMÁTICOS	Los delitos informáticos pueden definirse como cualquier acción u omisión que está legalmente tipificada y sancionada con una pena, y son llevados a cabo por una persona en el ámbito de la informática, con la consecuencia de causar perjuicio a individuos específicos y proporcionar beneficios ilícitos al autor del delito. Flores (2014)	Mediante el cuestionario sobre **delitos informáticos** se obtendrán datos, información para esta variable de estudio. Este instrumento constará de 10 reactivos que los colaboradores llenarán de forma anónima y lo más sinceramente posible.	INCREMENTO DE PHISHING COMO DELITO INFORMÁTICO .	1. ¿Considera que el phishing es actualmente uno de los delitos informáticos más frecuentes? 2. ¿Ha observado un aumento en las denuncias por phishing en los últimos años? 3. ¿Está de acuerdo en que el phishing debe considerarse un delito grave dentro del Código Penal peruano? 4. ¿Ha recibido usted o alguien de su entorno correos electrónicos sospechosos solicitando datos personales? 5. ¿Cree que los bancos y entidades financieras están aplicando medidas efectivas contra el phishing?	**SI** **NO**
			FRECUENCIA DEL FRAUDE INFORMÁTICO COMO DELITO INFORMÁTICO	6. ¿Cree usted que el fraude informático se ha convertido en uno de los delitos más comunes en el ámbito digital? 7. ¿Conoce casos cercanos de personas afectadas por fraudes informáticos? 8. ¿Considera que los delincuentes informáticos actúan con mayor frecuencia aprovechando el desconocimiento de los usuarios? 9. ¿Piensa que los fraudes informáticos están aumentando debido al fácil acceso a herramientas tecnológicas? 10. ¿Considera que las redes sociales son un canal frecuente para la comisión de fraudes informáticos?	**SI** **NO**

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES / INDICADORES	ITEMS	ESCALA DE MEDICIÓN
VARIABLE Y REGULACIÓN PENAL EN LA ERA DIGITAL	El derecho penal y procesal penal están experimentando una profunda transformación en la era digital, lo cual merece un tratamiento serio y responsable para hacer frente a los retos y desafíos contemporáneos. Por eso, es importante gestionar y fortalecer las competencias del profesional en la disciplina jurídica; además, para ampliar sus conocimientos, mejorar la asesoría y optimizar el patrocinio se debe perfeccionar la técnica jurídica, proponer la adaptación de las leyes a la complejidad de la criminalidad. Fernández (2024)	Mediante la encuesta sobre **regulación penal en la era digital** se rescatará información sobre esta variable de estudio; este instrumento estará comprendido por 10 reactivos orientados a las dimensiones e indicadores correspondientes, los colaboradores llenarán de forma anónima y lo más sinceramente posible.	CAPACIDAD DE RESPUESTA DEL SISTEMA PENAL	1 ¿Piensa que el sistema penal tiene suficientes herramientas tecnológicas para enfrentar el cibercrimen? 2. ¿Cree usted que las fiscalías están preparadas para investigar delitos informáticos con eficacia? 3. ¿Considera que la Policía Nacional cuenta con personal capacitado en delitos informáticos? 4. ¿Cree que los operadores de justicia reciben formación constante sobre criminalidad digital? 5. ¿Considera que las víctimas de delitos informáticos reciben una respuesta oportuna por parte de las autoridades?	**SI** **NO**
			EFICACIA NORMATIVA	6. ¿Considera que las normas penales vigentes en el Perú son eficaces para sancionar los delitos informáticos? 7. ¿Cree usted que la legislación penal actual está actualizada frente a las nuevas modalidades de delitos informáticos? 8 ¿Piensa que existen vacíos legales que dificultan la sanción de los delitos informáticos? 9. ¿Considera que el Código Penal peruano requiere reformas urgentes en materia de criminalidad informática? 10. ¿Cree usted que la normativa penal contempla adecuadamente la responsabilidad penal de los menores en delitos informáticos?	**SI** **NO**

CUESTIONARIO SOBRE DELITOS INFORMÁTICOS

ESTIMADO COLABORADOR: Saludos. El motivo de la presente es recoger datos e información objetiva para la tesis de **"LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024"**, este instrumento consta de 10 reactivos que deberás responder marcando alguna de las alternativas presentadas. Por favor, responde con objetividad. **ES ANÓNIMA, MUCHAS GRACIAS.**

Nº	ÍTEMS		
	PHISHING	**SI**	**NO**
01	¿Considera que el phishing es actualmente uno de los delitos informáticos más frecuentes?		
02	¿Ha observado un aumento en las denuncias por phishing en los últimos años?		
03	¿Está de acuerdo en que el phishing debe considerarse un delito grave dentro del Código Penal peruano?		
04	¿Ha recibido usted o alguien de su entorno correos electrónicos sospechosos solicitando datos personales?		
05	¿Cree que los bancos y entidades financieras están aplicando medidas efectivas contra el phishing?		
	FRAUDE INFORMÁTICO	**SI**	**NO**
06	¿Cree usted que el fraude informático se ha convertido en uno de los delitos más comunes en el ámbito digital?		
07	¿Conoce casos cercanos de personas afectadas por fraudes informáticos?		
08	¿Considera que los delincuentes informáticos actúan con mayor frecuencia aprovechando el desconocimiento de los usuarios?		
09	¿Piensa que los fraudes informáticos están aumentando debido al fácil acceso a herramientas tecnológicas?		
10	¿Considera que las redes sociales son un canal frecuente para la comisión de fraudes informáticos?		

CUESTIONARIO SOBRE REGULACIÓN PENAL

EN LA ERA DIGITAL

ESTIMADO COLABORADOR: Saludos. El motivo de la presente es recoger datos e información objetiva para la tesis de **"LOS DELITOS INFORMÁTICOS Y SU REGULACIÓN EN EL SISTEMA PENAL: UN ANÁLISIS DE LOS NUEVOS DESAFÍOS EN LA ERA DIGITAL DEL DISTRITO FISCAL DE ICA, AÑO 2024"**, este instrumento consta de 10 reactivos que deberás responder marcando alguna de las alternativas presentadas. Por favor, responde con objetividad. **ES ANÓNIMA, MUCHAS GRACIAS.**

Nº	ÍTEMS		
	CAPACIDAD	**SI**	**NO**
01	¿Piensa que el sistema penal tiene suficientes herramientas tecnológicas para enfrentar el cibercrimen?		
02	¿Cree usted que las fiscalías están preparadas para investigar delitos informáticos con eficacia?		
03	¿Considera que la Policía Nacional cuenta con personal capacitado en delitos informáticos?		
04	¿Cree que los operadores de justicia reciben formación constante sobre criminalidad digital?		
05	¿Considera que las víctimas de delitos informáticos reciben una respuesta oportuna por parte de las autoridades?		
	EFICACIA	**SI**	**NO**
06	¿Considera que las normas penales vigentes en el Perú son eficaces para sancionar los delitos informáticos?		
07	¿Cree usted que la legislación penal actual está actualizada frente a las nuevas modalidades de delitos informáticos?		
08	¿Piensa que existen vacíos legales que dificultan la sanción de los delitos informáticos?		
09	¿Considera que el Código Penal peruano requiere reformas urgentes en materia de criminalidad informática?		
10	¿Cree usted que la normativa penal contempla adecuadamente la responsabilidad penal de los menores en delitos informáticos?		

ANEXO 4: DATA DE RESULTADOS

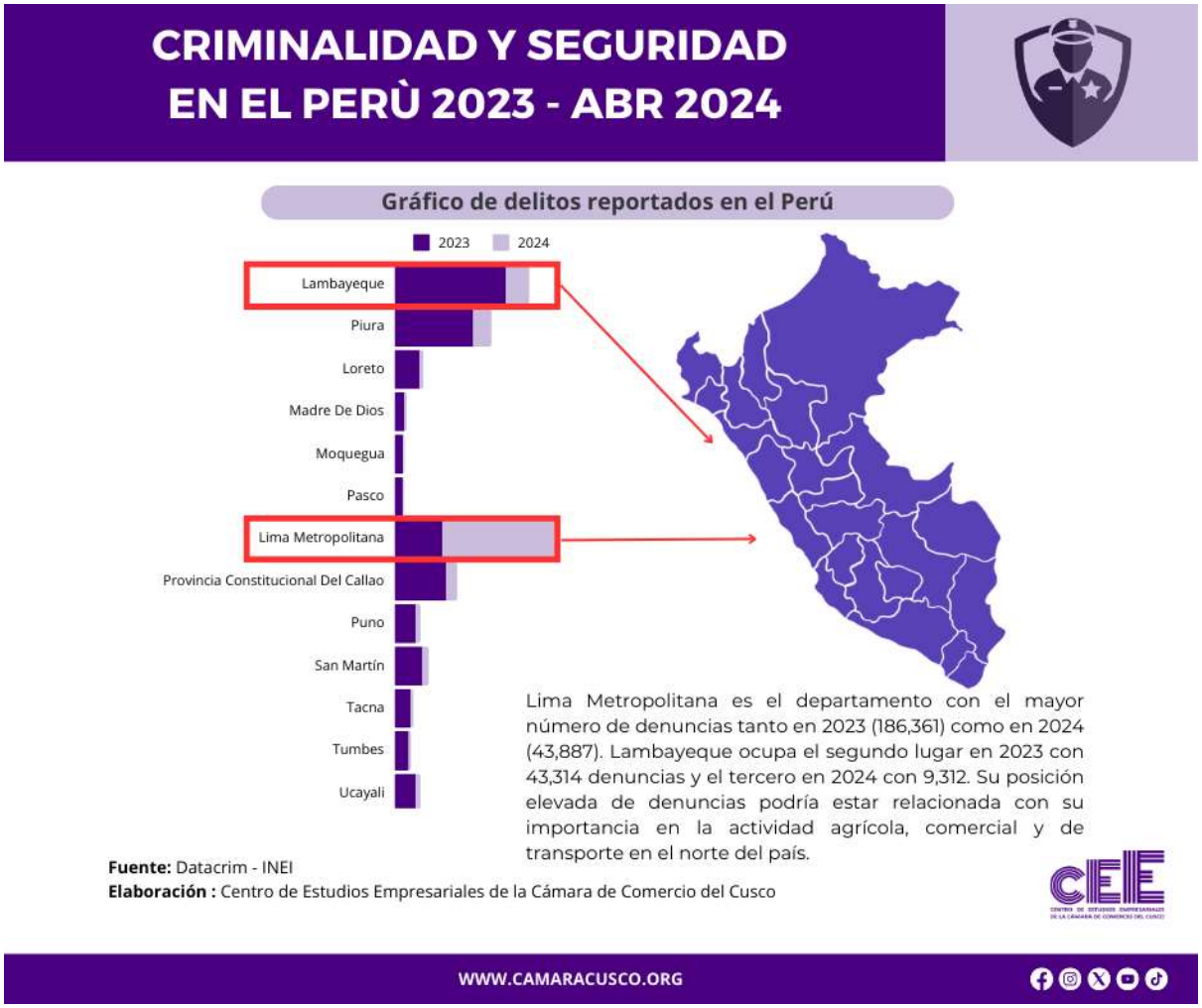
VX: DELITOS INFORMATICOS										
	D1: PHISHING					D2: CAPACIDAD				
	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10
1	1	1	1	1	2	1	1	1	1	1
2	1	1	1	1	2	1	1	1	1	1
3	1	1	1	1	2	2	1	1	1	1
4	1	1	1	1	2	2	1	1	1	1
5	1	1	1	1	2	1	1	1	1	1
6	1	2	1	1	2	1	1	1	1	1
7	1	2	1	1	2	1	1	2	1	1
8	1	2	1	1	2	1	1	1	1	1
9	1	2	2	1	2	1	2	1	1	1
10	1	2	2	1	2	1	2	1	1	1
11	1	2	2	1	2	2	2	1	1	1
12	1	2	1	1	2	2	2	1	1	1
13	1	1	1	1	2	2	1	1	1	1
14	1	1	1	1	2	1	1	1	1	1
15	1	1	1	2	2	1	1	1	1	1
16	1	1	1	2	2	1	1	1	2	1
17	1	1	2	2	1	1	1	1	2	1
18	1	1	1	2	1	1	1	1	1	1
19	1	1	1	2	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1	1
21	1	1	1	1	1	1	1	1	1	1
22	1	1	1	1	1	1	1	1	1	1
23	1	2	1	1	1	1	1	1	1	1
24	1	2	1	1	2	1	1	1	1	1
25	1	1	1	1	1	1	1	1	1	1
26	1	1	1	1	2	2	1	1	1	1
27	1	1	1	1	2	2	2	1	1	1
28	1	1	1	1	2	2	2	1	1	1
29	1	1	1	1	2	1	1	1	1	1
30	1	1	1	1	2	1	1	1	1	1
31	1	1	1	1	2	1	1	1	1	1
32	1	1	1	2	2	1	1	1	1	1
33	1	1	1	2	2	1	1	1	1	1
34	2	1	1	2	2	1	2	1	1	1
35	2	1	1	2	2	1	2	1	1	1
36	1	1	1	1	2	1	2	1	1	1
37	1	1	1	1	2	1	2	1	1	1
38	1	1	1	1	2	1	2	1	1	2

39	1	1	1	1	2	1	2	1	1	2
40	1	1	1	1	2	1	2	1	1	1
41	1	1	1	1	2	1	1	1	1	1
42	1	1	1	1	2	1	1	1	1	1
43	1	1	1	1	2	1	1	1	1	1
44	1	1	1	1	2	1	1	1	1	1
45	1	1	1	1	2	1	1	2	1	1
46	1	1	1	1	2	1	1	1	1	1
47	1	1	1	1	2	1	1	1	1	1
48	1	1	1	1	2	1	1	1	1	1
49	1	1	1	1	2	2	2	1	1	1
50	1	1	1	1	2	2	2	1	1	1
51	1	1	1	1	2	2	2	1	1	1
52	1	1	1	1	1	1	2	1	1	1
53	1	1	1	1	1	1	1	1	1	1
54	1	1	1	1	1	1	2	1	1	1
55	2	1	1	1	1	1	1	1	1	1
56	2	1	1	1	1	1	1	1	1	1
57	1	1	1	1	1	1	1	1	1	1
58	1	1	1	1	1	1	1	1	1	1
59	1	1	1	1	2	2	1	1	1	1
60	1	1	1	1	2	1	2	1	1	1
61	1	1	1	1	2	1	1	1	1	1
62	1	1	1	2	2	1	2	1	1	1
63	1	1	1	1	2	1	1	1	1	1
64	1	1	1	1	2	2	1	1	1	1
65	1	1	1	1	2	1	1	1	1	1
66	1	1	1	1	2	1	1	1	1	1
67	1	1	1	1	2	1	1	1	1	1
68	1	1	1	1	2	1	2	1	1	1
69	1	1	1	1	2	1	1	1	1	1
70	1	1	1	1	2	1	2	1	1	1
71	1	1	1	1	2	1	1	1	1	1
72	1	1	1	1	2	1	1	1	1	1
73	1	1	1	1	2	1	1	1	1	1
74	1	1	1	1	2	1	1	1	1	1
75	1	1	1	1	2	1	1	1	1	1
76	1	1	1	1	2	1	1	1	1	1
77	1	1	1	1	2	1	1	1	1	1
78	1	1	1	1	2	1	1	1	1	1
79	1	1	1	1	2	1	2	1	1	1
80	1	1	1	1	2	1	2	1	1	1

VY: REGULACIÓN PENAL EN LA ERA DIGITAL										
D1: FRAUDE INFORMATICO						D2: EFICACIA				
	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10
1	2	2	2	2	2	2	2	2	1	2
2	2	2	2	2	2	2	2	2	1	2
3	1	2	2	2	2	2	2	2	1	2
4	2	2	2	1	2	2	2	2	1	2
5	2	2	2	2	2	2	2	2	1	2
6	2	2	2	2	2	2	2	1	1	2
7	2	2	2	2	2	2	1	2	1	2
8	2	2	2	1	2	2	2	2	1	2
9	2	2	1	2	2	2	2	2	1	2
10	2	2	2	2	2	2	2	1	1	2
11	2	2	2	2	2	2	2	2	1	2
12	2	2	2	2	2	2	2	2	2	2
13	2	2	2	2	2	2	2	2	1	2
14	2	2	2	2	2	2	2	2	1	2
15	2	2	2	2	2	2	2	2	1	2
16	2	2	2	2	2	2	2	2	1	2
17	2	2	2	2	2	2	2	2	1	2
18	1	2	2	2	2	2	2	2	1	2
19	2	2	2	2	2	2	2	2	1	2
20	2	1	2	2	2	2	2	2	2	2
21	2	1	2	2	2	2	2	2	1	1
22	1	2	2	2	1	2	2	2	1	2
23	2	2	2	2	1	2	1	2	1	2
24	2	2	2	2	1	2	1	2	1	2
25	2	2	2	2	2	2	2	2	1	2
26	2	2	1	2	1	2	2	2	1	2
27	2	2	1	2	1	2	2	2	1	2
28	2	2	1	1	2	2	2	2	1	2
29	2	2	1	2	2	2	2	2	1	2
30	2	2	2	2	2	2	1	2	1	2
31	2	2	2	2	2	2	2	2	1	2
32	2	2	2	2	1	2	2	2	1	2
33	2	2	2	2	1	2	2	2	1	2
34	2	2	2	1	1	2	1	2	1	2
35	2	2	2	2	2	2	2	2	1	2
36	2	2	2	2	2	2	2	2	1	2
37	2	2	2	2	2	2	2	2	1	2
38	2	2	2	2	2	2	2	1	1	2
39	2	2	2	2	2	1	1	1	1	2
40	2	2	2	2	2	1	2	2	1	2

41	2	2	2	2	2	1	2	2	1	2
42	2	2	2	2	2	2	2	2	1	2
43	2	2	2	2	2	2	2	2	1	2
44	1	2	2	2	2	2	2	2	1	2
45	2	2	2	2	2	2	2	2	1	2
46	2	2	1	2	1	2	2	1	1	2
47	2	2	2	2	2	2	2	2	1	2
48	2	2	1	2	1	2	2	1	1	2
49	2	1	2	2	1	2	1	2	1	2
50	2	2	2	2	1	2	2	2	1	2
51	2	2	2	2	1	2	2	2	1	2
52	2	2	2	2	2	2	2	2	1	2
53	2	2	2	2	2	2	2	2	1	2
54	2	2	2	2	2	2	2	2	1	2
55	2	2	2	2	2	2	2	2	1	2
56	2	2	2	2	2	1	2	2	1	2
57	2	2	2	2	2	2	2	2	1	2
58	2	2	2	2	2	2	2	2	1	2
59	2	2	2	2	2	2	2	2	1	2
60	2	2	2	2	2	2	2	2	1	2
61	2	2	2	2	1	2	2	2	1	2
62	2	2	2	2	2	2	2	2	1	2
63	2	2	2	2	2	2	2	2	1	2
64	2	2	2	1	1	2	2	2	1	2
65	2	2	2	2	2	2	2	2	1	2
66	2	2	2	2	2	2	2	2	1	2
67	2	2	2	2	2	2	2	2	1	2
68	2	2	2	2	2	2	2	2	1	2
69	1	2	2	2	2	2	2	2	1	2
70	2	2	2	1	2	2	2	2	1	2
71	2	2	2	2	2	2	2	2	1	2
72	2	2	2	2	2	2	2	2	1	2
73	2	2	2	2	2	2	2	2	1	2
74	2	2	2	2	2	2	2	2	1	2
75	2	2	2	2	2	2	2	2	1	2
76	2	2	2	2	2	2	2	2	1	2
77	2	2	2	1	2	2	2	2	1	2
78	2	2	2	2	2	2	2	2	1	2
79	2	2	2	2	2	2	2	2	1	2
80	2	2	2	2	2	2	2	2	1	2

ANEXO 5: INFOGRAFIAS E INFORMACIÓN ALUSIVAS AL TEMA INVESTIGADO



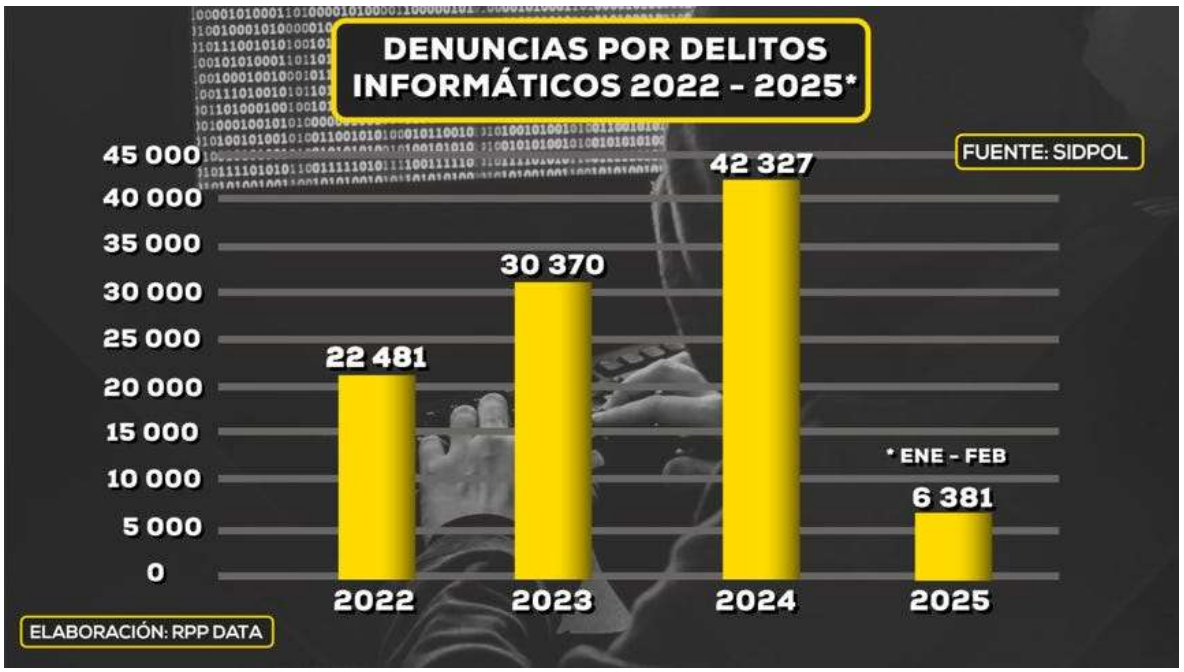
Fuente: *Datacrim – INEI*

Esta infografía de Criminalidad y Seguridad en el Perú ofrece una visión integral de la situación de la delincuencia en el país, proporcionando datos actualizados sobre los delitos reportados en diversas regiones y distintos departamentos. Este tipo de informe es fundamental para comprender las dinámicas delictivas, identificar áreas con mayores índices de criminalidad y orientar políticas públicas de seguridad.

Se destacan las regiones con mayores incidencias, como Lima Metropolitana y Lambayeque, que han registrado un alto número de denuncias tanto en 2023 como en 2024. Estos datos sugieren una correlación entre el crecimiento urbano, la actividad económica y los niveles de criminalidad.

El informe también pone de relieve la importancia de contar con información precisa para la toma de decisiones en materia de seguridad. Con esta información, las autoridades pueden

implementar estrategias más eficaces, focalizando los recursos en las zonas más afectadas y atacando las causas subyacentes de la criminalidad, como las condiciones socioeconómicas, el desempleo y la falta de acceso a servicios básicos. Este tipo de reporte no solo proporciona datos, sino que también subraya la necesidad de un enfoque integral para mejorar la seguridad pública.



Fuente: *RPP.*

Según el cuadro informativo, en 2024 se reportaron 42 mil denuncias por delitos informáticos en el Perú, lo que representa un aumento de casi el 40% a comparación del 2023, donde se reportaron 30 mil delitos. Las regiones con más casos fueron Lima Metropolitana con 23 mil casos, seguida de Piura (2 mil), La Libertad y Arequipa (1,900 cada una), Lambayeque y el Callao (1,500 cada una) e Ica con 1,200 denuncias.

El representante del Mininter indica que se están capacitando dentro de la PNP para atender el aumento de este tipo de delitos. "Si bien hoy día es más fácil cometer ese tipo de delitos, también es posible hacer ese rastreo de dónde van las cuentas, de cómo se mueven. Y es ahí donde también estamos trabajando para poder afinar la información y poder reaccionar a tiempo. Es un trabajo que va de la mano también con las leyes, con las normas, con los permisos que tiene que dar el Ministerio Público o el Poder Judicial", detalla.

Agrega además que están viendo una tendencia a la baja en el monto que se ha robado en lo que va del 2025. "Solo se ha reportado 3.45 millones de soles. Esto significa que ha bajado el nivel de denuncias del dinero robado [a comparación del año pasado], si esa tendencia sigue podríamos bajar en un 70% [de dinero sustraído]", estima Caso.

Si has sido víctima de algún delito informático, puedes denunciar llamando gratis al 1818 o al número (01) 431-8898, o acudir directamente la piso 9 de la Dirección de Investigación Criminal (Dirincri).

REPORTE DE DELITOS DENUNCIADOS RESPECTO AL DELITO DE ESTAFA AGRAVADA PARA SUSTRAER O ACCEDER A DATOS DE TARJETA DE AHORROS O CREDITO (ART. 196-A INC. 5) SEGÚN DISTRITO FISCAL A NIVEL NACIONAL

PERIODO: DEL 01 DE ENERO DEL 2021 AL 30 DE JUNIO DEL 2025

DISTRITO FISCAL	2021	2022	2023	2024	2025	Total general
AMAZONAS	3	11	4	2	6	26
ANCASH		2		3	2	7
APURIMAC		1	1	3	1	6
AREQUIPA	3	10	8	41	10	72
AYACUCHO	4	4	2	5	1	16
CAJAMARCA	4	3	21	18	6	52
CALLAO	8	6	7	5	2	28
CAÑETE	4	1	1	2	1	9
CUSCO	3	4	3	3	6	19
HUANCAVELICA	2	4	2		1	9
HUANUCO	13	8	3	8	2	34
HUAURA	13	13	24	24	11	85
ICA	38	58	57	27	37	217
JUNIN	7	1	1	7	7	23

Fuente: *La República*

Según la información que se muestra en el cuadro, las regiones con mayor número de denuncias son La Libertad con 108 casos, Lima Centro con 79 casos e Ica con 37 casos. Así también como Lambayeque con 34 casos y Piura con 14 casos. Asimismo, la modalidad de estafa agravada para sustraer datos de tarjetas de ahorro o crédito se ha vuelto cada vez más sofisticada. Explicó que esta situación se agravó desde la pandemia, ya que las operaciones financieras, tanto para pequeñas transacciones como para compras grandes, se realizan solo por medios digitales. “Así como la tecnología avanza en beneficio de las personas, también lo hace a favor de los delincuentes, que la utilizan para apropiarse ilegalmente de dinero”, señaló. Sobre las técnicas más comunes, la especialista detalló que los estafadores suelen hacer llamadas telefónicas para ofrecer pasajes aéreos a precios muy bajos para captar la atención de sus víctimas. Otra estrategia es el envío de enlaces falsos (phishing), en los que los usuarios son inducidos a ingresar sus datos personales y bancarios bajo el pretexto de acceder a ofertas o promociones.