Universidad Nacional
SAN LUIS GONZAGA

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"

FACULTAD DE DERECHO Y CIENCIA POLITICA

"AÑO DE LA RECUPERACION Y CONSOLIDACION DE LA ECONOMICA PERUANA"

....

EVALUACION DE ORIGINALIDAD

CONSTANCIA

El que suscribe, deja constancia que se ha realizado el análisis con el software de verificación de similitud TURNITIN ITHENTICATE 2.0 de **TESIS** titulada:

TRATAMIENTO POLITICO-NORMATIVO DEL FRAUDE INFORMATICO, DISTRITO FISCAL DEL CALLAO, 2020-2022

Presentado por:

JANAMPA SALAS, LISSETH FABIOLA

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 1% 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, 16 de Julio del 2025

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

Dra. ROSALINA TRAVEZAN MOREYRA
DIRECTORA

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA”

VICERRECTORADO DE INVESTIGACIÓN

Facultad de Derecho y Ciencia Política

Tratamiento político - normativo del fraude informático, Distrito Fiscal Del Callao, 2020-2022

Línea de Investigación

Sociedad, desarrollo sostenible, políticas públicas y ambientales.

TESIS

PARA OPTAR EL TÍTULO DE ABOGADO

AUTOR (A):

Bach. JANAMPA SALAS, LISSETH FABIOLA

Ica - Perú

2025

Dedicatoria

A mis padres,

Con profundo amor y mucha gratitud, dedico este logro a ustedes, cuya guía y apoyo han sido mi faro constante. Gracias por enseñarme el valor de la perseverancia y por brindarme las herramientas para enfrentar cada desafío.

A mi hermano, gracias por estar siempre allí, en los momentos buenos y malos, demostrando que el camino es más fácil cuando se comparte.

Este trabajo es el fruto de muchas enseñanzas recibidas dentro y fuera de casa, y cada página refleja la sabiduría y amor que ustedes me han impartido.

Agradecimiento

Quiero expresar mi más sincero agradecimiento a todas las personas que han contribuido a la realización de este trabajo. En primer lugar, a mi asesora, Mg. Perpetua Emelia Rodriguez Vega, cuya experiencia, paciencia y dedicación fueron esenciales para el desarrollo de esta investigación. Su guía crítica y alentadora me ha permitido crecer académicamente y personalmente.

A mis compañeros de estudio, gracias por compartir tantas horas de estudio y por todas las experiencias que juntos hemos vivido durante este viaje académico. Cada uno de ustedes ha dejado una marca imborrable en mi memoria.

Agradezco también al personal docente de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional “San Luis Gonzaga de Ica”, por su disposición y apoyo en cada etapa de mi formación académica.

Finalmente, mi gratitud a mi familia: a mis padres y a mi hermano, por su amor y soporte constante. Sin su presencia y su apoyo, este camino habría sido mucho más difícil de recorrer.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

El estudio planteó determinar la relación entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022, en donde la investigación fue de tipo básica, considerando el empleo del cuestionario para obtener datos de 81 operadores de justicia. Los resultados indicaron que el tratamiento político normativo mostró una relación de 0.788 frente al fraude informático, al enfocarse en establecer lineamientos para identificar y sancionar prácticas engañosas, lo que fortalece la seguridad en el uso de plataformas digitales. La Ley N° 30096 presentó una relación de 0.691, abordando las sanciones frente a accesos indebidos, promoviendo así un entorno virtual seguro. El delito informático tuvo una relación de 0.731, facilitando la tipificación de infracciones y limitando la impunidad. La tecnología de la información alcanzó una relación de 0.779, destacando la importancia de sistemas robustos que protejan los datos y contrarresten la manipulación indebida. Se ha concluido que el enfoque de políticas normativas, en conjunto con legislaciones específicas y el desarrollo tecnológico, contribuye de manera significativa a reducir la incidencia del fraude informático, fortaleciendo la confianza en el entorno digital. Además, la regulación y control de las actividades ilícitas mejoran la seguridad de los sistemas, promoviendo un espacio virtual más seguro y controlado.

Palabras claves: Tratamiento, política, normas, fraude informático, delito informático.

Abstract

The study aimed to determine the relationship between political-normative treatment and computer fraud, Callao Fiscal District, 2020 - 2022, where the research was of a basic type, considering the use of the questionnaire to obtain data from 81 justice operators. The results indicated that the political-normative treatment showed a relationship of 0.788 compared to computer fraud, by focusing on establishing guidelines to identify and sanction deceptive practices, which strengthens security in the use of digital platforms. Law No. 30096 presented a relationship of 0.691, addressing sanctions against improper access, thus promoting a safe virtual environment. Computer crime had a relationship of 0.731, facilitating the classification of infractions and limiting impunity. Information technology reached a relationship of 0.779, highlighting the importance of robust systems that protect data and counteract improper manipulation. It has been concluded that the regulatory policy approach, together with specific legislation and technological development, contributes significantly to reducing the incidence of computer fraud, strengthening confidence in the digital environment. In addition, the regulation and control of illicit activities improve the security of systems, promoting a safer and more controlled virtual space.

Keywords: Treatment, policy, regulations, computer fraud, computer crime.

I. Introducción

A nivel internacional, según el Convenio de Ciberdelincuencia de Europa, reveló que en los últimos años el 81.4% del total de delitos cometidos, corresponden a los delitos informáticos y/o cibernéticos, los cuales, pese a la existencia de normativas interpuestas, estas presentan vacíos legales. México, también registra cifras altas en delitos informáticos, los cuales últimamente vienen siendo cometidos mediante SMiShing, donde su tratamiento a este delito es ineficaz, dado a la falta de preparación y capacitación en los ministerios públicos (Carrera, 2021).

En el mundo, los delitos cibernéticos han deteriorado los modelos de seguridad, ocasionando un gran incremento de víctimas, donde ante dicho problema, los gobiernos a nivel global vienen efectuando esfuerzos mediante normativas y políticas cibernéticas bajo un marco legal (Espinoza, 2022). En Ecuador un estudio indicó que los fraudes informáticos se realizan masivamente en agravio a todo tipo de empresas, siendo el phishing o malware uno de los tipos de fraudes más cometidos en los últimos años (De la Cruz y Llulli, 2023).

Por otro lado, la expansión respecto al empleo de sistemas informáticos, así como los de telemática en escenarios tanto público como privado tiende favorecer directamente a la práctica delictiva de cualquier delito y/o fraude, convirtiéndose en un nuevo espacio que facilita su maniobra, frente a esta problemática, en los estados mundiales vienen regulando sus políticas instauradas, como en el caso de Puerto Rico, dado que es uno de los países con mayores delitos informáticos en un 91%; mientras que, el cibercrimen en Latinoamérica y Caribe representa el 50% (Lujan, 2022).

A nivel nacional, según el Ministerio Público en el 2022 señaló que las fiscalías provinciales penales, han venido registrando un significativo acrecentamiento en este delito, siendo así que en el 2021 cerca de 57.63% delitos informáticos fueron registrados, mientras que, en el 2022 estos aumentaron a un 72.74 %, situación que afectando al país y socavando la confianza. Frente a ello, es que se vienen implementando técnicas basada en inteligencia artificial (AI), a fin de hacer un mejor tratamiento normativo y penal a este tipo de delitos (Chumbe, 2023).

Asimismo, en nuestra normativa penal sea esta sustantiva y/o especial no se hallan reguladas tales escenarios de hecho, dado que sólo se hallan detalladas de forma general dentro del delito de fraude informático; las mismas que son acciones que se efectúan en un sistema informático a fin de adquirir un provecho ilícito, no obstante, tales verbos detallados (clonar, alterar, introducir, etc.) no amparan hechos como la creación de “URLS falsas” de las financieras, uso de software malicioso y demás; resultando crucial la regulación y tratamiento de tales situaciones de hecho de forma específica (Custodio, 2021).

En el ambiente regional, un estudio reveló que la ciberdelincuencia constantemente está avanzando en su comisión, sin embargo, en ocasiones no está sancionado por la Ley de Delitos Informáticos Ley

30096 y la Ley 30171, cuyo propósito es defender a la sociedad; el problema incurre en al acrecentamiento de actos delictivos en el espacio virtual, trayendo consigo un incremento representativo de denuncias por el delito de fraude informático, las cuales en varias ocasiones no son tratadas debidamente por el Ministerio Público (Malca, 2023).

El Distrito Fiscal del Callao se enfrentó a desafíos significativos en el ámbito del fraude informático durante el periodo 2020-2022. Las causas fundamentales incluyen la insuficiente regulación tecnológica y la falta de actualización en las normativas legales, lo cual genera un ambiente propicio para la proliferación de actividades fraudulentas. Como consecuencia, se observa un incremento notable en los delitos cibernéticos, lo que impacta negativamente en la seguridad financiera y la confianza pública. Los principales problemas identificados abarcan la incapacidad para detectar y prevenir fraudes de manera efectiva, la falta de recursos especializados para investigar estos delitos, y la carencia de protocolos adecuados para la gestión de incidentes informáticos. Esta problemática institucional pone en riesgo la integridad de la información y la estabilidad económica de los afectados, generando un clima de incertidumbre y vulnerabilidad.

En referencia con lo expuesto, la **pregunta general** fue ¿Cuál es la relación entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022? Además, las **preguntas específicas** fueron ¿Cuál es la relación entre la dimensión Ley N° 30096 y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022? ¿Cuál es la relación entre la dimensión delito informático y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022? ¿Cuál es la relación entre la dimensión tecnología de la información y comunicación y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022?

La incidencia de fraude informático en el Callao ha generado serias repercusiones en la seguridad y confianza de la ciudadanía. Este tipo de delitos no solo afecta a las víctimas directas, sino que también tiene un impacto negativo en la percepción de seguridad de toda la **sociedad**. Además, las pérdidas económicas y la violación de la privacidad contribuyen a un ambiente de desconfianza generalizada. La necesidad de abordar esta problemática es fundamental para restaurar la integridad de las instituciones y proteger a los ciudadanos de futuros perjuicios.

En referencia con la **justificación práctica,** la generación de información a través de este estudio proporcionó una base sólida para que investigadores y profesionales interesados diseñen programas eficaces de compensación y prevención del fraude informático. Al analizar las causas y consecuencias de estos delitos, se facilitó la identificación de áreas críticas que requieren atención. Esta información fue esencial para el desarrollo de políticas y medidas concretas que puedan ser implementadas por diversas entidades, contribuyendo a mitigar el impacto del fraude y fortalecer la seguridad digital en el ámbito fiscal y más allá.

Este estudio contribuyó a llenar un **vacío significativo en el conocimiento** actual sobre el tratamiento político y normativo del fraude informático. La investigación se enfocó en aspectos que han sido subestimados en estudios previos, ofreciendo una nueva perspectiva y aportando datos empíricos que enriquecen el campo académico. La exploración de los mecanismos legales y políticos en la lucha contra el fraude proporciona una comprensión más amplia y detallada, que puede servir como base para futuros estudios y teorías en esta área.

En cuanto a la **justificación metodológica,** este estudio se basó en la recopilación exhaustiva de datos mediante cuestionarios aplicados a operadores de justicia. La metodología empleada aseguró una recolección de información precisa y relevante, permitiendo un análisis detallado de los factores involucrados en el fraude. La elección de esta técnica garantizó que se obtenga una visión integral de la problemática, basada en la experiencia y conocimientos de profesionales en el campo, lo que facilitó la obtención de resultados que reflejan la realidad del entorno estudiado.

La **importancia** de este estudio radicó en su capacidad para abordar una problemática crítica que afecta tanto a las instituciones como a los ciudadanos del Callao. Al enfocarse en el fraude informático, la investigación destacó la urgencia de implementar medidas efectivas para combatir este tipo de delitos. Los hallazgos obtenidos tienen el potencial de influir en la formulación de políticas públicas y en la mejora de las estrategias de seguridad digital, beneficiando a la comunidad en general y fortaleciendo la confianza en las instituciones.

Bajo lo referenciado, el **objetivo general** fue: Determinar la relación entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022. De igual forma, los **objetivos específicos** fueron: 1) Establecer la relación entre la dimensión Ley N° 30096 y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022; 2) Establecer la relación entre la dimensión delito informático y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022; 3) Establecer la relación entre la dimensión tecnología de la información y comunicación y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022.

Así mismo, la **hipótesis general** fue: Existe relación significativa entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022. Cabe reconocer que, las **hipótesis específicas** fueron: 1) Existe relación significativa entre la dimensión Ley N° 30096 y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022; 2) Existe relación significativa entre la dimensión delito informático y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022; 3) Existe relación significativa entre la dimensión tecnología de la información y comunicación y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022.

En complemento con lo expuesto, los **antecedentes** quedaron en evidencia del siguiente modo:

Calva y Nivelo (2021), Ecuador, se enfocaron en estudiar el tratamiento de los delitos informáticos (DI) según el código orgánico penal. Se desarrolló una indagación analítica, explicativa, exploratoria, empírica, documental, cualitativa, se consideró la observación. Los resultados ostentaron que, para el tratamiento eficaz de DI desde que son denunciados hasta ser juzgados se requiere capacitación más permanente para jueces, fiscales, peritos, y demás operadores de justicia; también se necesita dotación de infraestructura y tecnología adecuada, así como convenios internacionales que contribuyan a perseguir este tipo de fraudes. Se concluyó que, existe desconocimiento en el tratamiento de los DI, por lo que la mayoría de estos no son juzgados debidamente.

Díaz (2023), Ecuador, se enfocó en estudiar los desafíos legales frente a los delitos informáticos (DI). Se desempeñó un estudio explicativo, analítico, cualitativo, documental, no experimental. Los resultados ostentaron que, en el ambiente ecuatoriano se necesita mayor capacitación, así como concienciación, esencialmente en los operadores judiciales y el bancario, dado que así se podrá abordar de forma eficaz estos crímenes. Concluyendo que, se requiere una mejor adaptación a la legislación, dado que los desafíos de los ciberdelitos son cada vez más frecuentes y demandan de un mejor tratamiento.

Cuellar y Astaiza (2024), Colombia, buscaron realizar un estudio dogmático de los delitos de fraude informático en Colombia. Se trabajó una indagación analítica, exploratoria, documental, explicativa, cualitativa, se desarrolló un análisis documental. Los resultados exhibieron que, la creación de legislaciones en el marco penal ha contribuido que en Colombia se luche de forma eficaz contra este delito, permitiendo que las autoridades y demás especialistas, actúen y otorguen un mejor tratamiento a este delito. Concluyendo que, la lucha contra este delito y la protección de la información es crucial para que desarrollo digital en Colombia.

Delgado (2022), Chimbote, se enfocó en estudiar el tratamiento penal (TP) de los delitos informáticos (DI) contra el patrimonio de las personas jurídicas y naturales. Se efectuó una indagación cuantitativa, transversal, analítica, explicativa, se consideró la aplicabilidad de un cuestionario con 50 especialistas. Los resultados exhibieron que, el 70% consideró que el avance de las TICS acrecentó este delito; el 50% dijo que no hay eficacia de la ley para penar estos delitos; el 67.5% señaló que no hay prevención de las entidades bancarias para penar este delito. Concluyendo que, el TP de los DI contra el patrimonio viene siendo deficiente, dado que no se percibe dentro de FI todos los tipos de estos delitos contra el patrimonio.

Ramos y Salvador (2022), Huaraz, examinar la regulación de las nuevas modalidades del delito informático en la Ley N° 3009, así como su modificatoria. Se trabajó una indagación explicativa, cualitativa, analítica, transversal, se consideró la aplicación de una entrevista con 5 fiscales. Los resultados exhibieron que, la delictiva conducta del Smishingen en el país suele ser constante, dado que

un número representativo de los ciudadanos cuenta con aplicativos de mensajería, los cuales son un medio idóneo que accede al cometido del acto ilícito. Concluyendo que, las modalidades nuevas respecto al delito informático requieren ser incorporadas para que sean sancionadas dentro de la Ley de Delitos Informáticos.

Alcántara (2024), Pimentel, buscó examinar la ley 30096 y su aplicación a los delitos de fraude informático en el país. Se trabajó una indagación explicativa, cualitativa, analítica, se consideró la aplicación de una encuesta con 50 especialistas. Los resultados revelaron que, el 60% indicó que existen vacíos legales dentro de la ley 30096 y el 40% indicó que no; el 70% mencionó que si se requieren mejores especialistas en ciberdelitos en el país y el 30% señaló que re requiere capacitación a los fiscales en el tema; el 70% indicó se necesita mejor conocimiento informático; el 80% señaló que las conductas ilícitas afectan lo sistemas informáticos; el 60% indicó que no se cumple con la garantía de la lucha contra la ciberdelincuencia. Concluyendo que, en la ley 30096 se halló vacíos legales, por lo que el delito examinado no es debidamente condenado.

Tacuche (2023), Lima, se enfocó en examinar sí los actos de investigación son suficientes para el tratamiento normativo (TN) en los delitos de fraude informático (DFI). Se trabajó una indagación explicativa, cualitativa, analítica, no experimental, se consideró la aplicabilidad de un análisis documental. Los resultados ostentaron que, se buscó establecer que las indagaciones realizadas en las diligencias iniciales no son suficientes para la aclaración e identificación de los sujetos culpables por las denuncias de los DFI, resultando crucial una serie de medidas, con la intención de aminorar la impunidad, al igual que la capacitación técnica de los persecutores y actores intervinientes. Concluyendo que, los actos de investigación no vienen siendo suficientes para un mejor TN en los DFI.

La estructuración del estudio investigativo se desarrolló de la siguiente manera: El primer segmento se centró en el planteamiento principal, exponiendo los antecedentes, metas y justificación del trabajo. A continuación, la segunda fase detalló los métodos utilizados para la recopilación y análisis de datos. El tercer apartado se dedicó a los descubrimientos obtenidos durante la indagación. Posteriormente, la cuarta parte contrastó estos resultados con investigaciones previas. En la quinta sección, se resumieron los objetivos alcanzados. El sexto segmento propuso recomendaciones para enfrentar los desafíos identificados. Finalmente, la séptima sección registró las fuentes bibliográficas consultadas, y la última parte incluyó los anexos que respaldan el proyecto.

II. Estrategia metodológica

Tipo de investigación

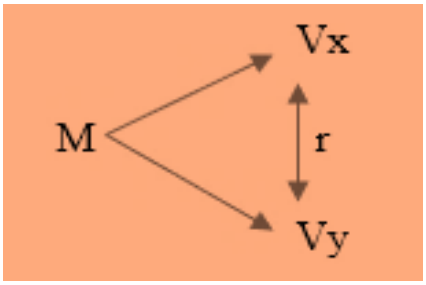
Se planteó una investigación básica que se orientó principalmente a la recopilación de datos con el objetivo de enriquecer el entendimiento y el conocimiento sobre el tópico analizado. Según Guillén et al. (2020), la exploración científica se centra en ahondar en el tema para impulsar el desarrollo de nuevos conocimientos.

Enfoque de investigación

Se empleó una metodología cuantitativa para este estudio, utilizando datos medibles para lograr una descripción detallada y precisa de los elementos analizados. Guillén et al. (2020) señalan que el uso de cifras es crucial para alcanzar respuestas exactas a los objetivos planteados. Este enfoque se centró en metas cuantificables, permitiendo una descripción concreta de los componentes estudiados mediante técnicas estadísticas.

Nivel de investigación

Se utilizaron métodos estadísticos en este estudio correlacional para recolectar datos que demuestren la relación entre las variables. La información obtenida ilustró cómo interactúan y se comportan conjuntamente los fenómenos analizados. De acuerdo con Guillén et al. (2020), las herramientas estadísticas son esenciales para revelar la interconexión de las variables, proporcionando una comprensión detallada de su dinámica.



Se recopilaron las opiniones del grupo "M" para examinar eficazmente la interacción entre las variables "Vx" y "Vy", demostrando así la relación "R" existente entre ellas.

Diseño de investigación

Para preservar las características y comportamientos de los elementos en su entorno natural, se empleó un diseño no experimental. Este garantizó una representación precisa de los fenómenos observados sin modificaciones. Evaluar los elementos en su contexto original, sin la intervención del investigador,

permitió obtener una visión auténtica y sin alteraciones de las situaciones estudiadas. Según Guillén et al. (2020), este método asegura una observación fiel y sin modificaciones.

Población y Muestra

Población

En el Distrito Fiscal del Callao, se eligió a 81 operadores de justicia accesibles y con conocimiento en el tema. Este grupo brindó información y perspectivas fundamentales, lo cual permitió una evaluación y comprensión detallada del contexto investigado. Según Guillén et al. (2020), esta selección facilitó una caracterización exhaustiva del área analizada.

Muestra

Como el grupo es inferior a cien individuos, se escogió una muestra censal no probabilística de 81 operadores de justicia del Ministerio Público. Esta selección cubrió toda la población objetivo, asegurando la inclusión de todos los operadores pertinentes para el análisis. Este tipo de muestra es apropiado cuando no se necesitan métodos estadísticos para seleccionar a los participantes, especialmente si la población es menor de cien personas, de acuerdo con Guillén et al. (2020).

Muestreo

Para facilitar la selección de participantes que ofrezcan datos de alta calidad, se establecieron criterios precisos para un muestreo intencional. Esta técnica aseguró una recopilación detallada y relevante de información de los individuos seleccionados, mejorando significativamente el análisis del contexto. Guillén et al. (2020) afirman que este enfoque garantiza la obtención de información significativa de los sujetos elegidos.

Criterios de inclusión

Para la muestra, se seleccionaron a los operadores de justicia en funciones y autorizados dentro del Distrito Fiscal en estudio. Estos participantes debieron proporcionar su consentimiento informado oral, garantizando así su participación voluntaria en la investigación. La selección se enfocó en aquellos que cumplan con los criterios establecidos y que acepten voluntariamente formar parte del estudio.

Criterios de exclusión

No se incluyeron en el estudio los expertos que no tengan conocimientos relevantes sobre el tema o no entreguen su consentimiento informado. También fueron excluidos aquellos que no demuestren interés en participar. La selección se enfocó en profesionales que cumplan con estos criterios, garantizando así la relevancia y la participación voluntaria de los elegidos.

Técnicas de recolección de datos

Mediante encuestas con preguntas estructuradas, se recogieron las opiniones de la muestra sobre la problemática en estudio. Esta técnica permitió evaluar y caracterizar detalladamente la situación analizada, basándose en las respuestas proporcionadas por el grupo seleccionado. De acuerdo con Guillén et al. (2020), este método facilitó una comprensión profunda del contexto investigado.

Instrumentos de recolección de datos

Se aplicó un cuestionario que contiene 15 preguntas sobre el tratamiento político normativo y otras 10 dirigidas al fraude informático. Este instrumento permitió a los participantes expresar sus opiniones, facilitando así la caracterización de los fenómenos analizados. De acuerdo con Guillén et al. (2020), este cuestionario se enfoca en un contexto específico para el análisis.

Validez del instrumento

En relación con esta investigación, se optó por emplear hojas técnicas del instrumento, las cuales funcionaron como método de verificación para garantizar la excelencia del contenido. El autor basó su trabajo en este procedimiento para asegurar que la estructura del aparato de recopilación de información fuera de alta calidad (consulte el Anexo 6). De acuerdo con Guillén et al. (2020), la comprobación de la excelencia es una tarea que el investigador debe llevar a cabo, apoyándose en las contribuciones teóricas de autores que han colaborado en la creación del instrumento.

Confiabilidad del instrumento

El estudio ha demostrado una fiabilidad notable en las variables analizadas, ya que cada evaluación arrojó un coeficiente de consistencia interna superior a 0.70 (ver Anexo 8). Guillén et al. (2020) respaldan este enfoque, definiéndolo como la confirmación de la estabilidad interna de una herramienta, lo que garantiza la confiabilidad de los datos recolectados.

Tabla 1

Confiabilidad por Alfa de Cronbach

Variable	Confiabilidad	Condición
Variable 1	0.943	
Variable 2	0.909	Confiable
Ambas variables	0.957	

Técnicas de procesamiento, análisis e interpretación de datos

Para ilustrar los resultados, se emplearon métodos de estadística descriptiva, utilizando frecuencias y porcentajes para describir los fenómenos. Se generaron gráficos y tablas para una representación clara

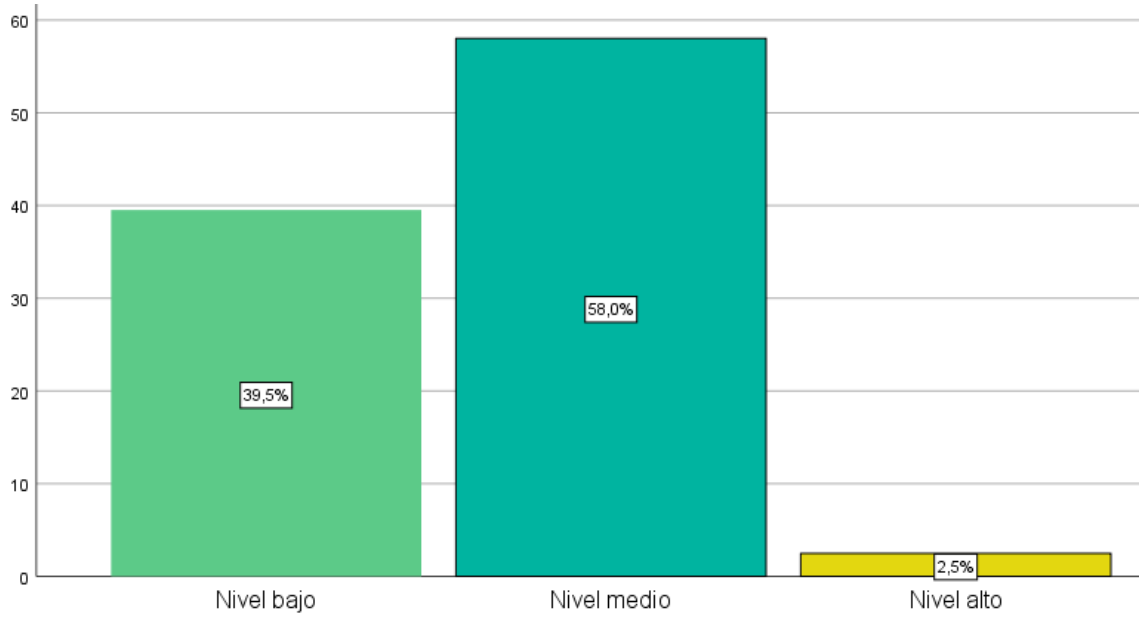
de los datos. Además, se aplicó estadística inferencial para calcular correlaciones y determinar la significancia, facilitando la comprensión de las interrelaciones entre las variables. La hipótesis se validó con un nivel de significancia menor a 0.05. Los datos fueron analizados utilizando Excel y SPSS versión 26.00.

III. Resultados

Estadística descriptiva de variables y dimensiones

Figura 1

Análisis de la variable Tratamiento político - normativo

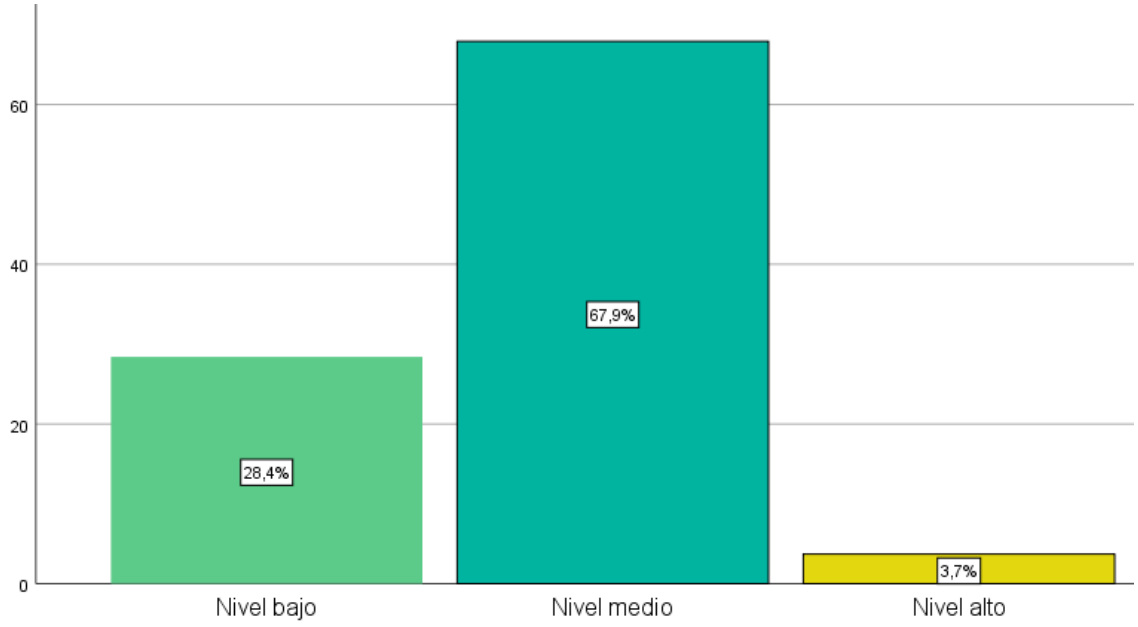


Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 58.00%, debido a que, los esquemas normativos se desarrollan en respuesta a la evolución de prácticas ilícitas, el proceso regulatorio incorpora enfoques específicos que apuntan a prevenir y sancionar actividades en el entorno digital. Los actores encargados de la creación y revisión de las normativas requieren considerar las distintas aristas de los actos no autorizados en la esfera digital para implementar directrices precisas que disminuyan las brechas legales. Así, se establecen estrategias y medidas que buscan alinear el orden normativo con las innovaciones tecnológicas, reflejando una conexión directa entre el análisis político y la implementación de políticas efectivas en este ámbito.

Figura 2

Análisis de la dimensión Ley N° 30096

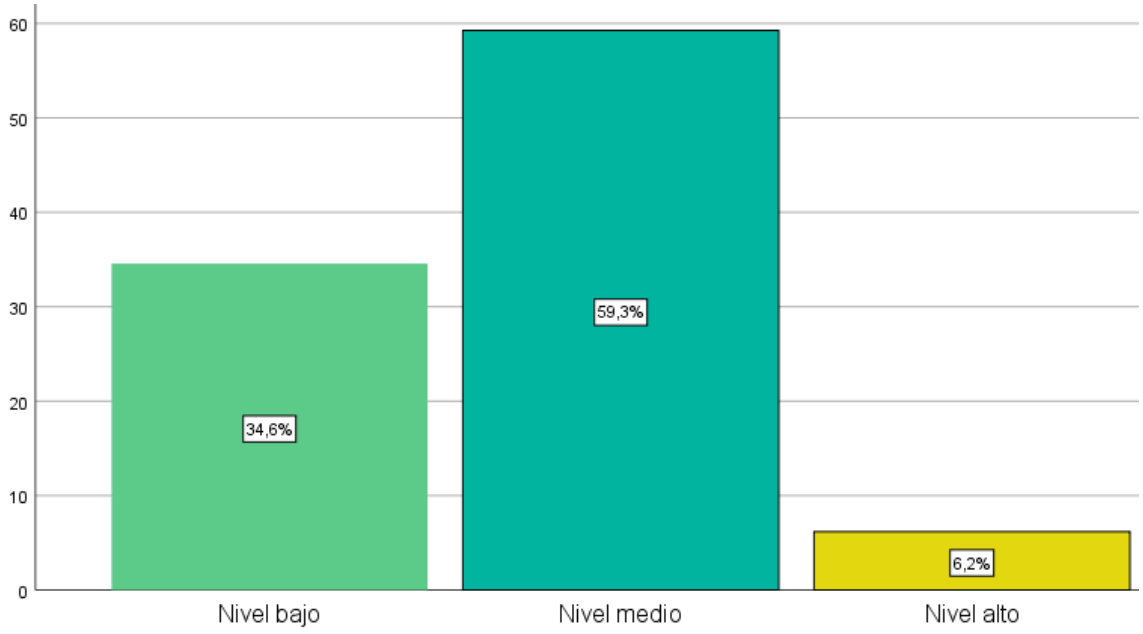


Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 67.90%, debido a que, la normativa estipulada en la Ley N° 30096 busca enfrentar actos delictivos en entornos digitales, esta regula de manera explícita acciones que pueden comprometer la integridad y seguridad de la información en el ciberespacio. Esta legislación refleja una respuesta concreta ante el avance de delitos asociados a nuevas tecnologías, proporcionando herramientas y sanciones para contener el desarrollo de infracciones electrónicas. La ley promueve un marco de seguridad digital mediante directrices detalladas, orientadas tanto a la prevención como a la penalización de aquellos que transgreden los límites de la legalidad en el ámbito virtual.

Figura 3

Análisis de la dimensión Delito informático

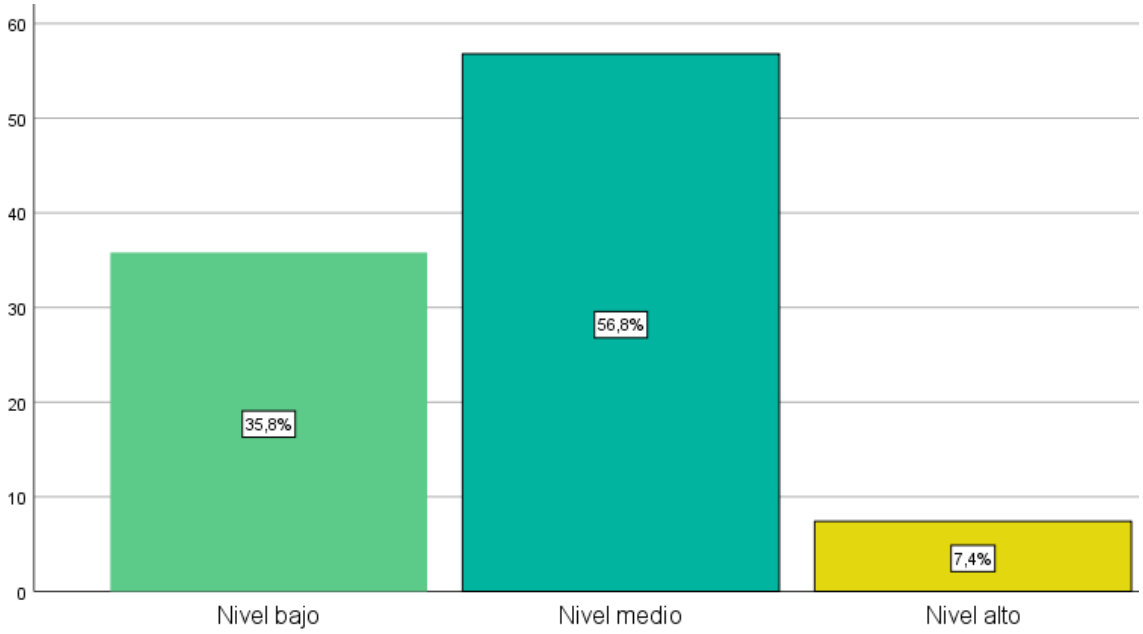


Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 59.30%, debido a que, los actos ilegales en el entorno digital presentan una complejidad creciente, el marco normativo se adapta continuamente para abordar conductas no permitidas en espacios virtuales. Estas infracciones requieren de una normativa actualizada que permita enfrentar las distintas técnicas y métodos empleados por actores que buscan vulnerar sistemas electrónicos. La inclusión de términos específicos en la regulación busca no solo sancionar, sino también disuadir la proliferación de actos no autorizados en la red, ajustándose a las transformaciones tecnológicas y a los métodos emergentes de intervención en plataformas digitales.

Figura 4

Análisis de la dimensión Tecnología de la información y comunicación

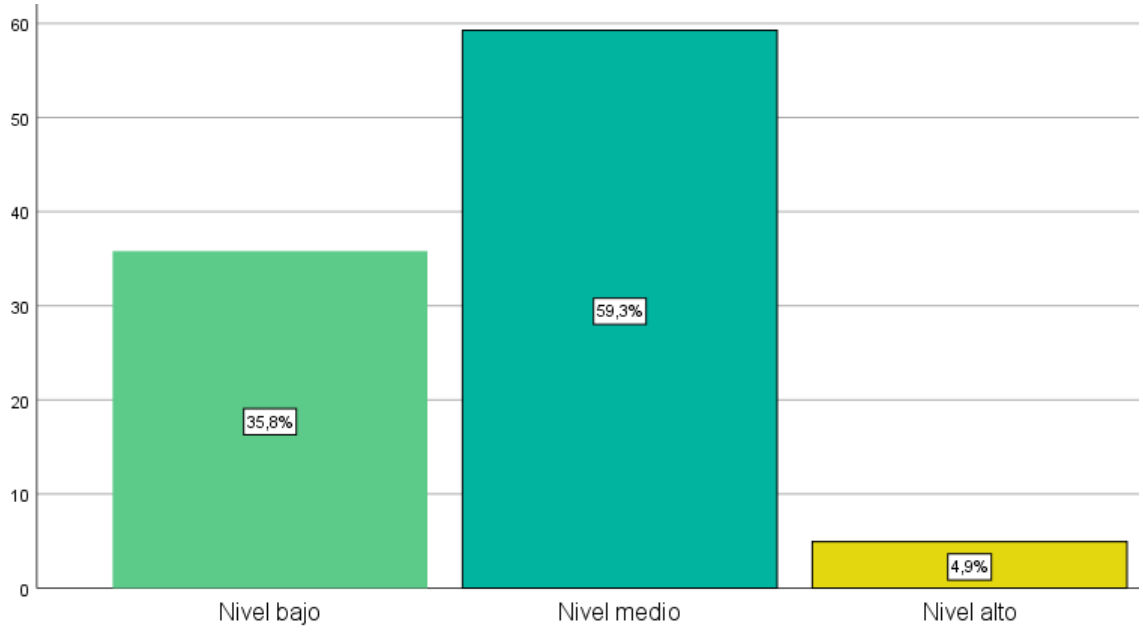


Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 56.80%, debido a que, las herramientas tecnológicas constituyen el núcleo de las infraestructuras digitales, la regulación en este ámbito reconoce su rol tanto en el fortalecimiento de la protección de datos como en la prevención de prácticas no autorizadas. Estas tecnologías proporcionan el contexto y los medios que deben regularse para salvaguardar la información y garantizar el uso legítimo de las plataformas electrónicas. De esta manera, las políticas y normas se diseñan para proteger tanto a los usuarios como a las organizaciones de prácticas ilegales que afectan el flujo de datos y su confidencialidad.

Figura 5

Análisis de la variable Fraude informático

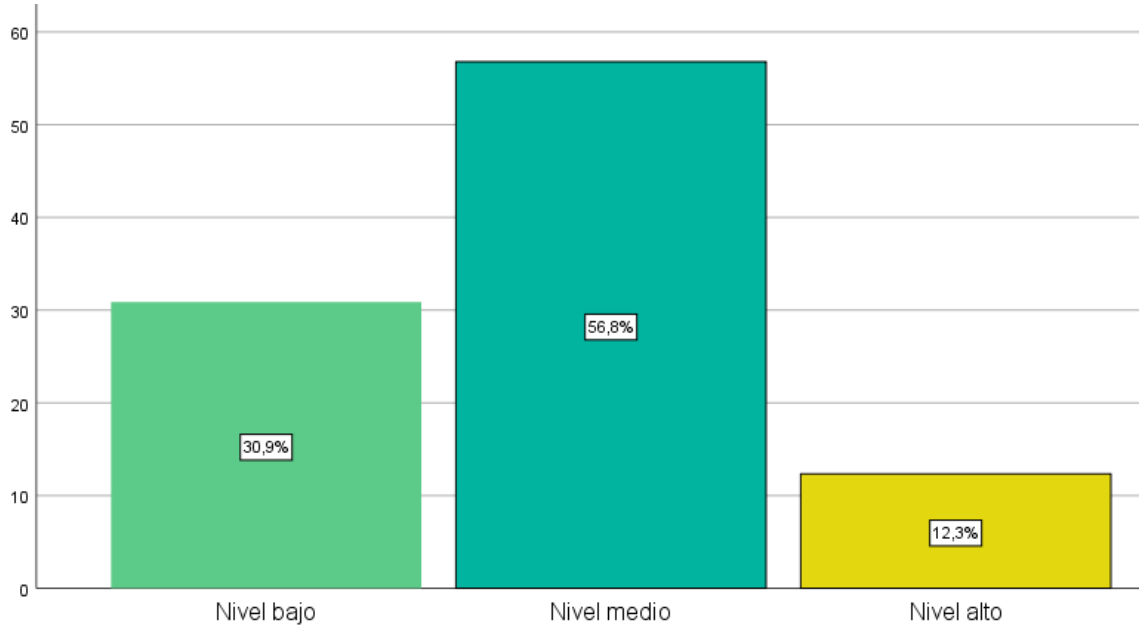


Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 59.30%, debido a que, las tácticas para desviar o manipular información en el entorno electrónico evolucionan constantemente, el marco regulatorio debe enfocarse en identificar y tipificar estas prácticas de forma exhaustiva. Las regulaciones buscan capturar las particularidades de estas actividades y desincentivar su ejecución mediante sanciones adecuadas. Este tipo de estrategias permite establecer barreras contra la proliferación de técnicas engañosas y fomenta un ambiente digital más seguro, protegiendo tanto a individuos como a organizaciones contra posibles pérdidas o accesos indebidos a sus recursos electrónicos.

Figura 6

Análisis de la dimensión Tratamiento normativo

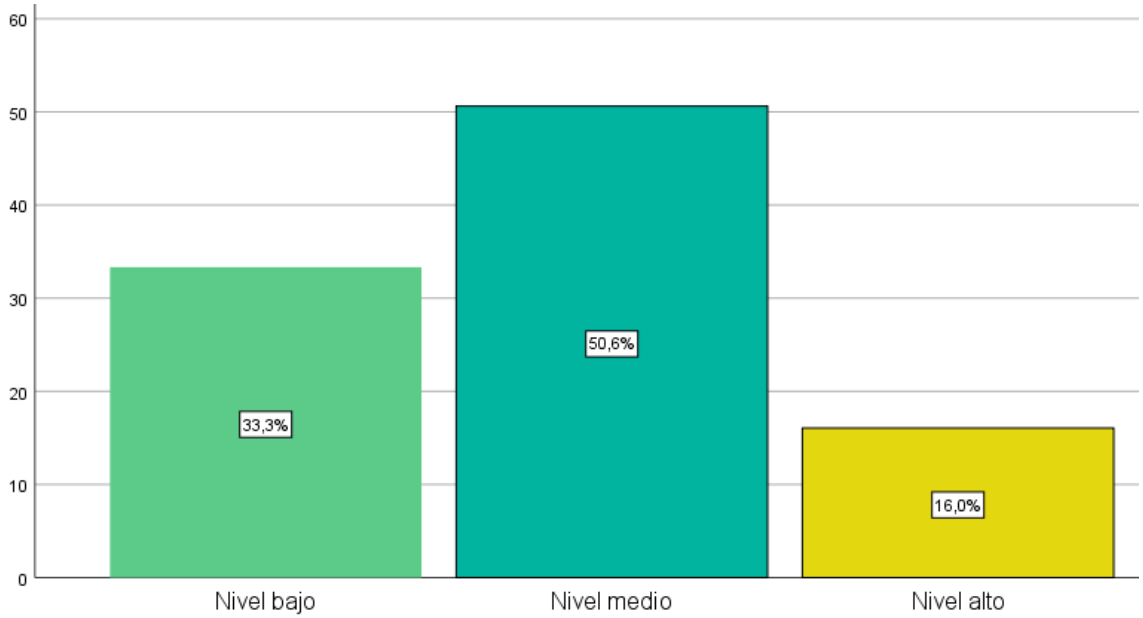


Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 56.80%, debido a que, el proceso de reglamentación orientado a la protección en entornos digitales demanda un enfoque detallado y adaptable, la legislación se ajusta a los nuevos escenarios de vulnerabilidad que surgen con el tiempo. Esta normatividad considera las distintas maneras en que las infracciones pueden desarrollarse, diseñando medidas de control específicas para cada contexto. A través de una regulación progresiva y ajustada a los cambios tecnológicos, se garantiza la protección de la integridad y confidencialidad en los espacios de intercambio digital, promoviendo un uso seguro de estos medios.

Figura 7

Análisis de la dimensión Modalidades



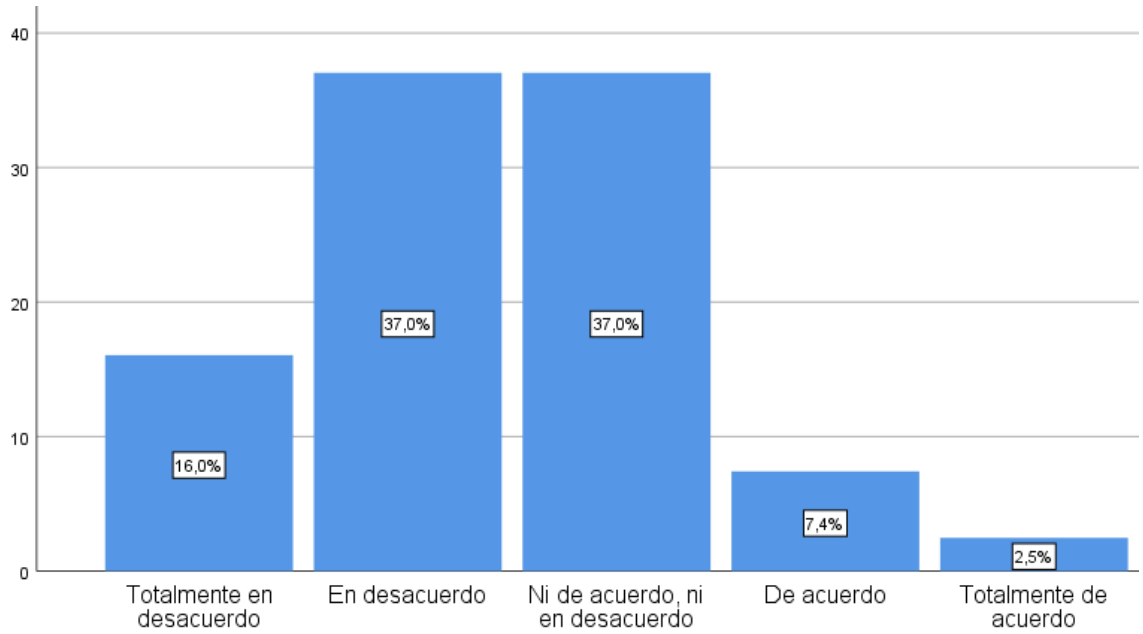
Nota: Procesado en SPSS V 26.00

El nivel de tendencia prevalente fue el medio con un valor del 50.60%, debido a que, existen múltiples formas de intervención no autorizada en el ciberespacio, el análisis normativo incorpora una clasificación detallada de las diferentes técnicas empleadas en estos actos ilícitos. Cada modalidad es identificada y descrita en función de sus características y mecanismos, permitiendo una respuesta regulatoria específica. Este enfoque diversificado facilita la aplicación de sanciones apropiadas y medidas de prevención, asegurando que el marco normativo aborde con precisión las variantes y desafíos que presentan los métodos utilizados para manipular o acceder ilegalmente a la información.

Estadística descriptiva por pregunta

Figura 8

¿Considera que la Ley N° 30096 ha sido adecuadamente implementada para abordar los desafíos del fraude informático en el contexto peruano?

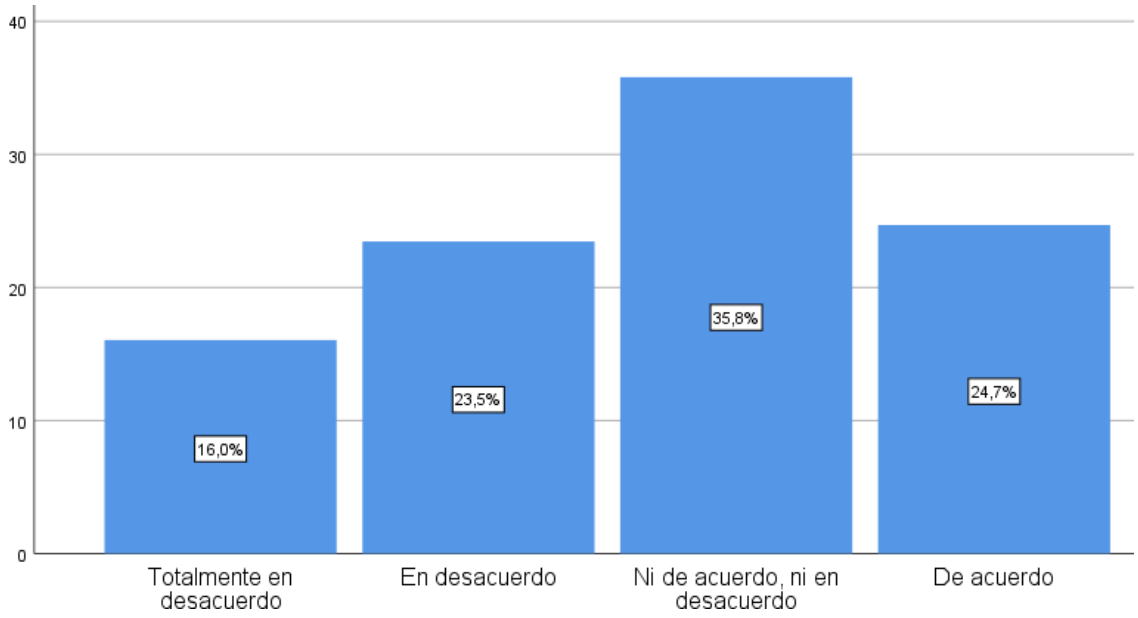


Nota: Procesado en SPSS V 26.00

Con un 37.00% de los encuestados posicionándose en un estado neutral, el análisis sugiere una percepción ambigua respecto a la efectividad en la implementación de la Ley N° 30096 en el contexto específico de delitos informáticos. Este dato refleja una posible falta de claridad o resultados visibles en la aplicación de la ley, lo cual podría indicar la necesidad de reforzar aspectos específicos de la regulación o de optimizar los procedimientos actuales. Al no existir una inclinación notable hacia acuerdo o desacuerdo, se evidencia una postura que requiere intervenciones que aborden inquietudes no definidas en torno a la ejecución y el alcance de la ley en la práctica.

Figura 9

¿Cree que las actuales regulaciones y políticas bajo la Ley N° 30096 se están cumpliendo de manera efectiva para prevenir el fraude informático?

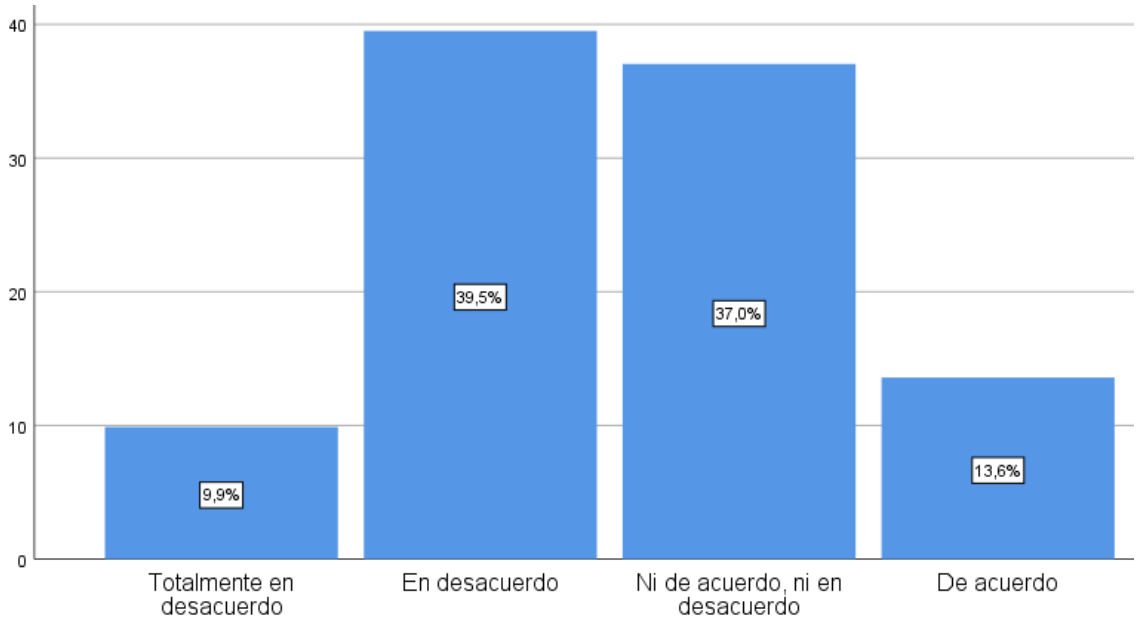


Nota: Procesado en SPSS V 26.00

Con un 35.80% de los participantes que mantienen una postura neutral, se observa una percepción de incertidumbre sobre la eficacia en el cumplimiento de las regulaciones actuales bajo la Ley N° 30096 para mitigar los fraudes de naturaleza digital. Esta posición refleja una posible inconsistencia entre la normativa y su aplicación práctica, lo cual podría indicar carencias en los mecanismos de supervisión o en los recursos asignados para su cumplimiento efectivo. La falta de una respuesta clara podría sugerir que la ley no ha logrado generar la confianza suficiente en la población para percibirla como una herramienta completamente funcional en la prevención de estos delitos.

Figura 10

¿Opina que las autoridades competentes han proporcionado suficientes recursos y formación para garantizar la correcta implementación de la Ley N° 30096 en la lucha contra el fraude informático?

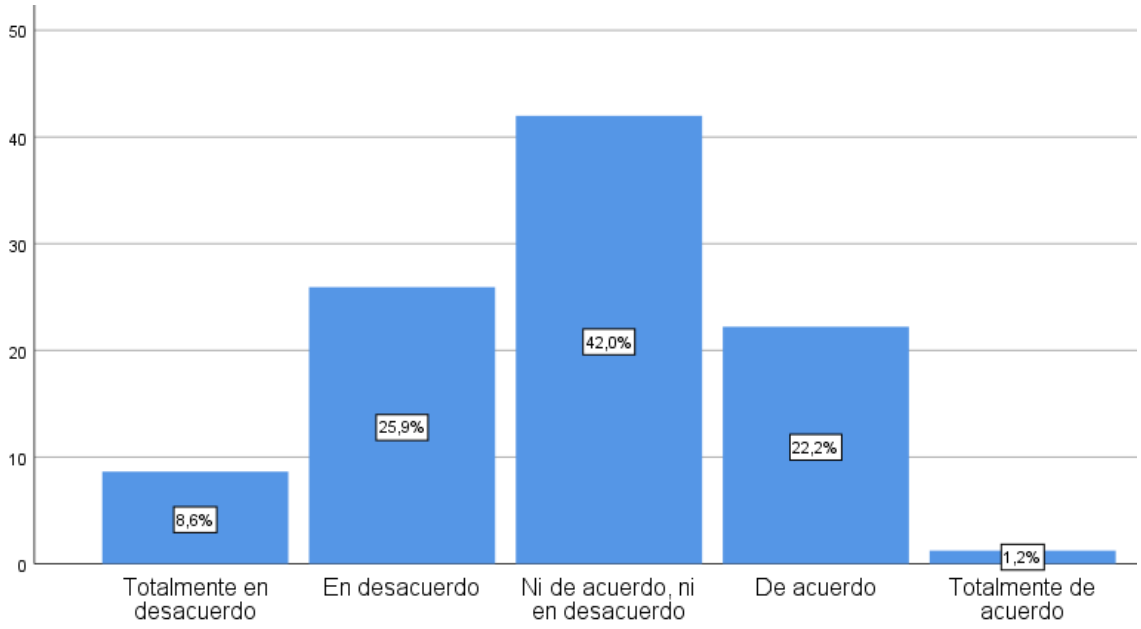


Nota: Procesado en SPSS V 26.00

El 39.50% en desacuerdo refleja una percepción negativa respecto a la provisión de recursos y la capacitación de los responsables para la implementación efectiva de la Ley N° 30096. Este valor sugiere que las autoridades no están cumpliendo de manera efectiva con las expectativas de apoyo y formación necesarias, lo que podría estar afectando el impacto esperado de la ley en la lucha contra los delitos informáticos. La falta de acuerdo general sobre el soporte ofrecido puede estar vinculada con una insuficiencia en recursos o en programas de formación, lo cual afecta directamente la ejecución eficaz de la normativa.

Figura 11

¿Estima que las sanciones contempladas en la Ley N° 30096 son adecuadas y se están aplicando de manera justa para disuadir las prácticas de fraude informático?

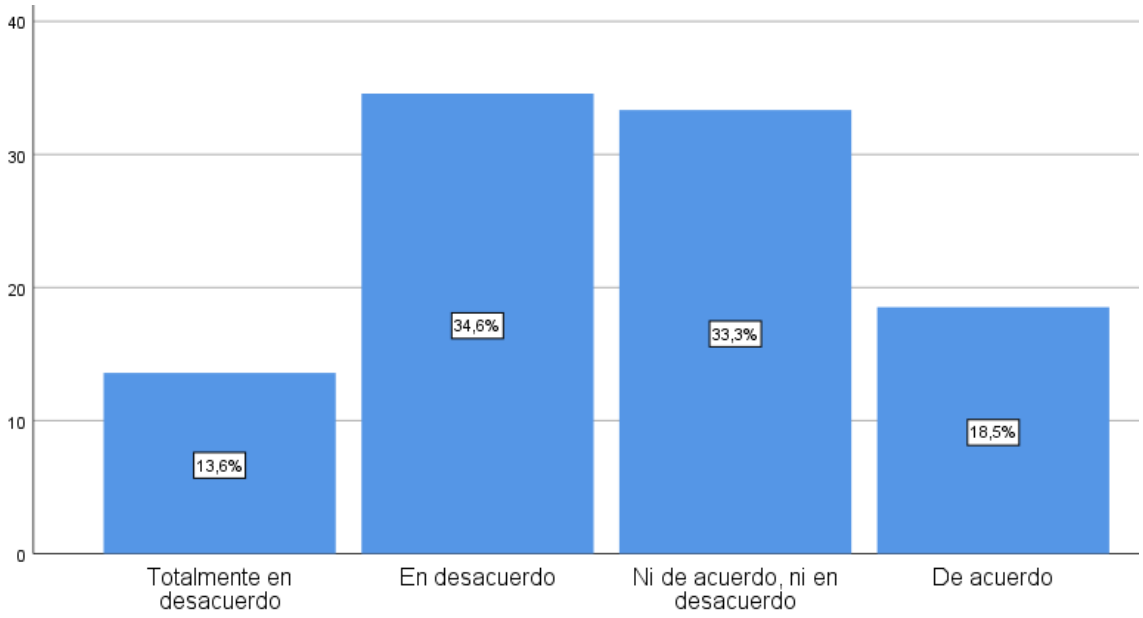


Nota: Procesado en SPSS V 26.00

Un 42.00% de neutralidad sobre la adecuación y aplicación de sanciones para disuadir los fraudes indica una percepción mixta, que podría reflejar una falta de convencimiento en cuanto a la efectividad de las sanciones vigentes. Esta postura sugiere que, aunque las sanciones están establecidas, su impacto disuasorio no es evidente para una porción significativa de la población, lo cual podría estar relacionado con una percepción de aplicabilidad inconsistente o con insuficiente severidad de las penalidades. Este dato evidencia una necesidad potencial de revisar la estructura y aplicación de las sanciones en la ley.

Figura 12

¿Juzga que la Ley N° 30096 incluye suficientes mecanismos de actualización para adaptarse a las nuevas modalidades de fraude informático que surgen con los avances tecnológicos?

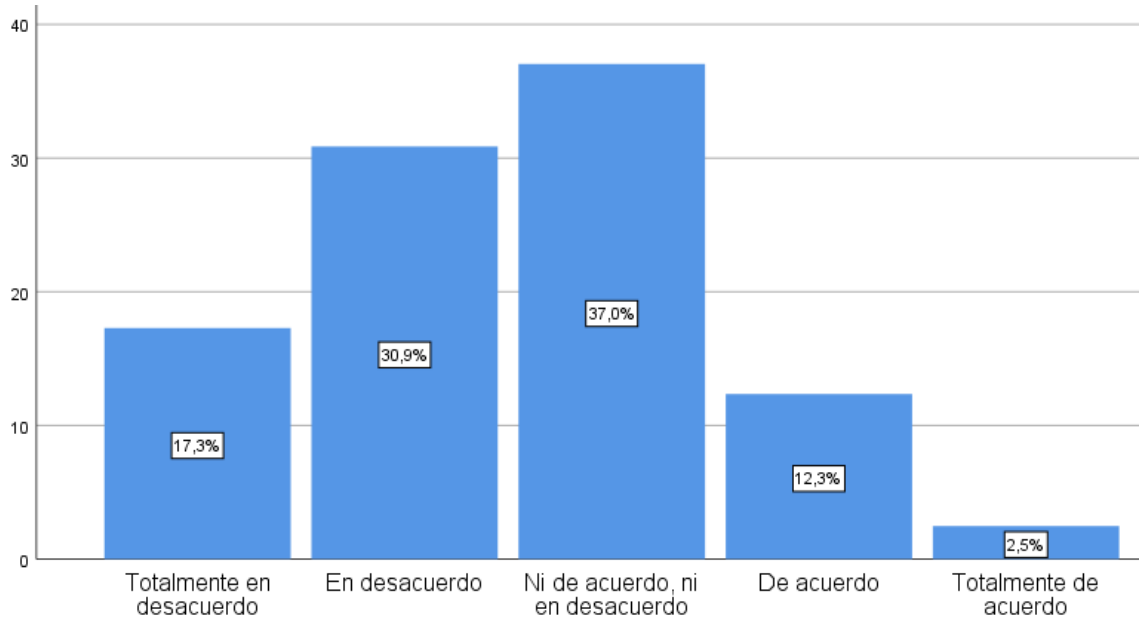


Nota: Procesado en SPSS V 26.00

La postura de desacuerdo en el 34.60% respecto a los mecanismos de actualización de la Ley N° 30096 señala una percepción crítica hacia la capacidad de la normativa para adaptarse a nuevas modalidades de fraude. Este resultado podría implicar que las disposiciones legales actuales no están avanzando al ritmo de las innovaciones tecnológicas, lo que limita su efectividad y su capacidad de respuesta frente a los métodos emergentes de fraude. Una falta de actualización en la normativa genera dudas sobre su vigencia y pertinencia en un entorno en constante evolución.

Figura 13

¿Considera que la actual legislación en torno al delito informático es suficiente para reducir de manera significativa la incidencia de fraudes cibernéticos en el país?

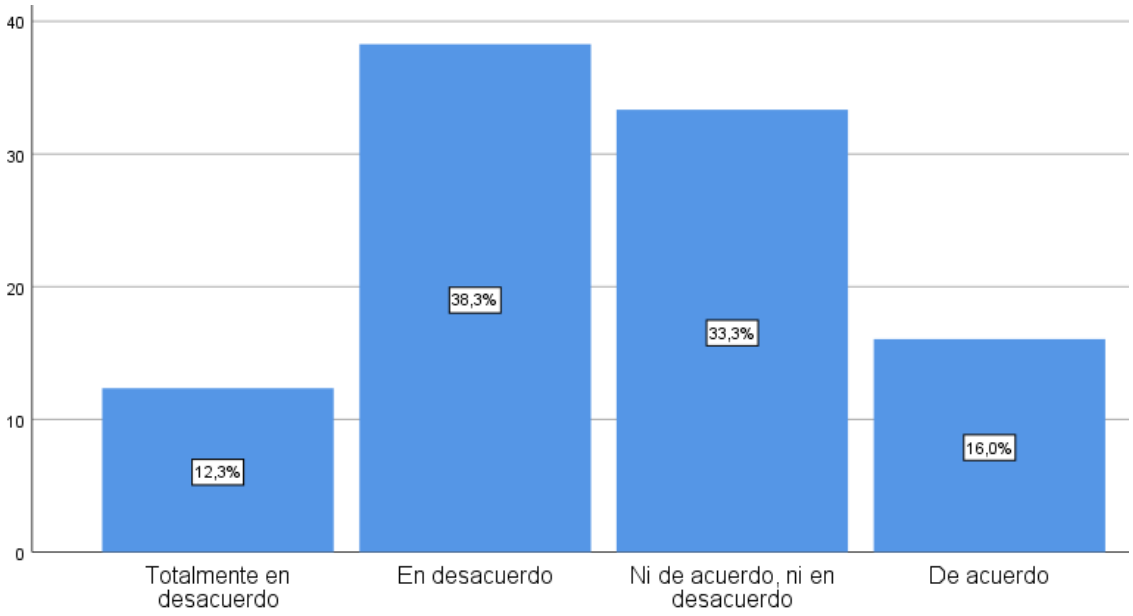


Nota: Procesado en SPSS V 26.00

Un 37.00% de neutralidad en cuanto a la suficiencia de la legislación refleja dudas sobre la capacidad de las normativas actuales para impactar en la reducción de fraudes cibernéticos. Esta postura indica que, aunque las leyes están en vigor, la percepción de su impacto en la reducción de estos delitos sigue siendo ambigua, posiblemente debido a una falta de resultados visibles o de una implementación efectiva. Esta respuesta sugiere que la legislación no está alcanzando el impacto preventivo que se esperaría en un contexto digital.

Figura 14

¿Cree que las medidas normativas implementadas son adecuadas para proteger las infraestructuras críticas y minimizar la explotación de vulnerabilidades en el ámbito informático?

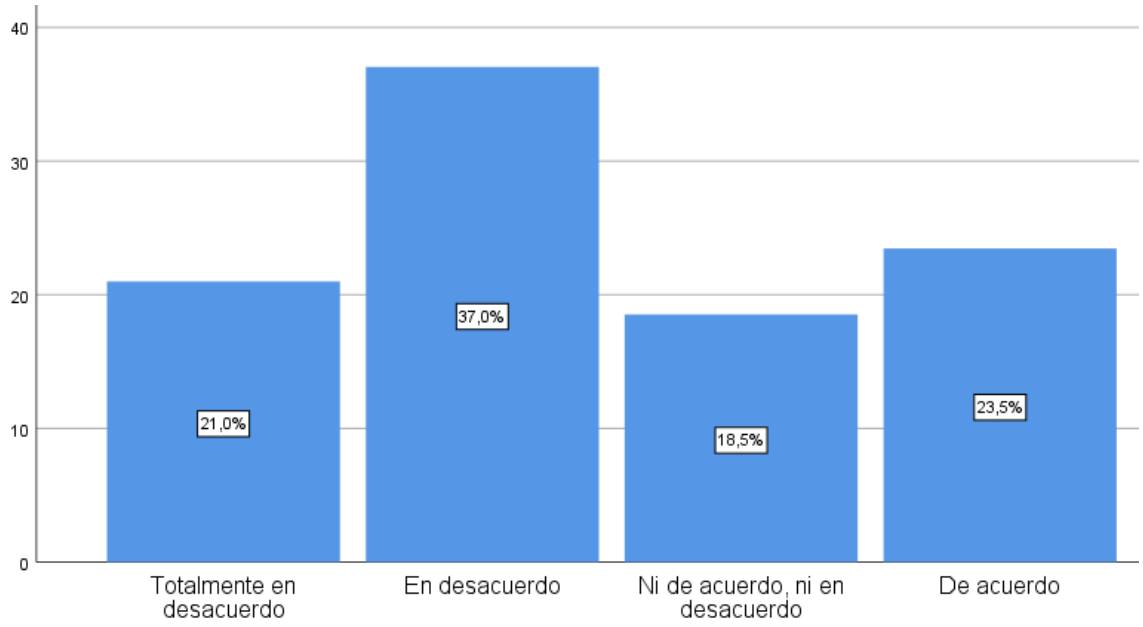


Nota: Procesado en SPSS V 26.00

La percepción negativa en el 38.30% respecto a las medidas para proteger infraestructuras críticas indica una opinión desfavorable sobre la capacidad actual para resguardar componentes esenciales contra posibles ataques. Este desacuerdo podría estar relacionado con la insuficiencia de recursos o de estrategias preventivas eficaces que aseguren la protección de dichas infraestructuras. La falta de confianza en la protección ofrecida señala una necesidad de fortalecer las medidas en cuestión y asegurar que estas respondan a las vulnerabilidades emergentes del entorno tecnológico.

Figura 15

¿Opina que las políticas actuales de combate contra el delito informático han logrado una disminución efectiva en la frecuencia de estos delitos?

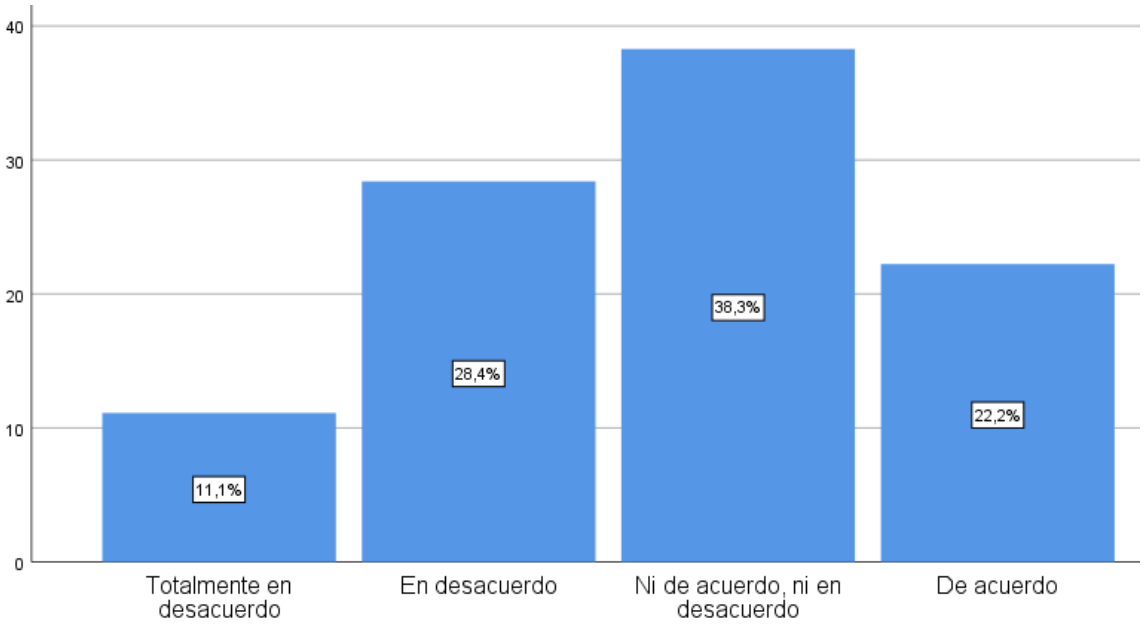


Nota: Procesado en SPSS V 26.00

El 37.00% en desacuerdo sobre la disminución de delitos informáticos sugiere una percepción de ineficacia de las políticas actuales en la contención de estos crímenes. Este resultado indica que los esfuerzos legislativos y las políticas implementadas no parecen estar generando un efecto disuasivo suficiente, y podría señalar que existen brechas significativas en la aplicación o en el enfoque de las políticas, afectando la percepción pública sobre la seguridad y la prevención en el entorno digital.

Figura 16

¿Juzga que las estrategias adoptadas por el gobierno para fortalecer la ciberseguridad son efectivas para prevenir la explotación de vulnerabilidades en los sistemas informáticos?

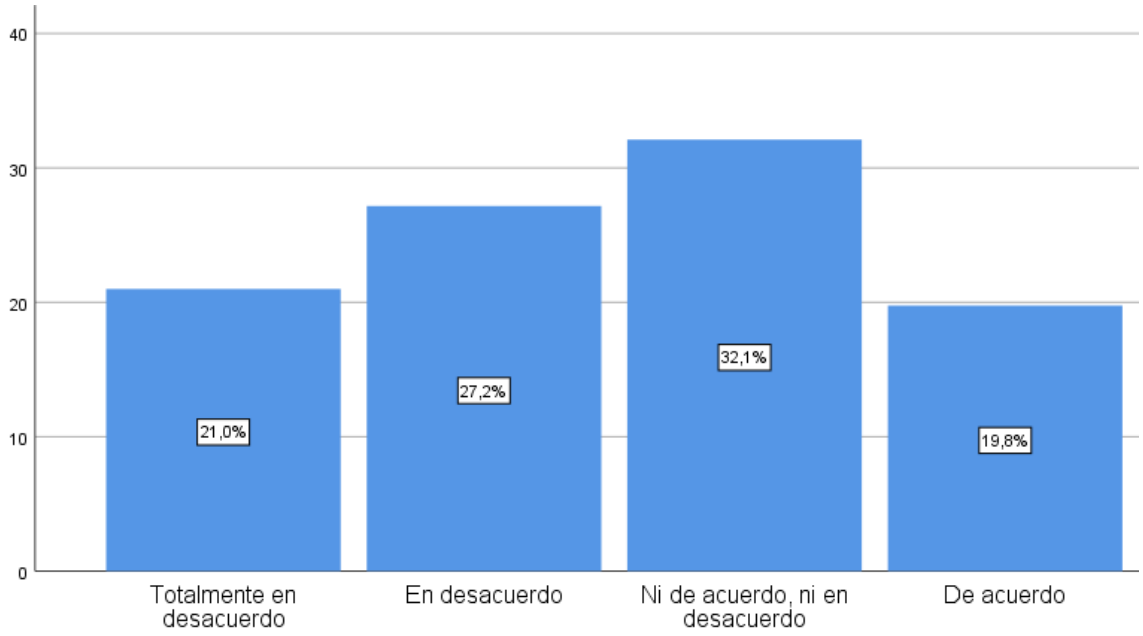


Nota: Procesado en SPSS V 26.00

Un 38.30% de respuestas neutrales en cuanto a la efectividad de las estrategias gubernamentales para prevenir vulnerabilidades en sistemas informáticos refleja una percepción de incertidumbre en la robustez de estas medidas. Este valor podría sugerir que los esfuerzos actuales no logran transmitir un impacto tangible en la protección de la infraestructura digital, lo que puede estar ligado a limitaciones en la implementación o a una percepción de insuficiencia en las medidas propuestas para abordar los riesgos inherentes a la tecnología.

Figura 17

¿Estima que el marco legal vigente es suficientemente robusto para hacer frente a la evolución constante de las técnicas utilizadas en el fraude informático?

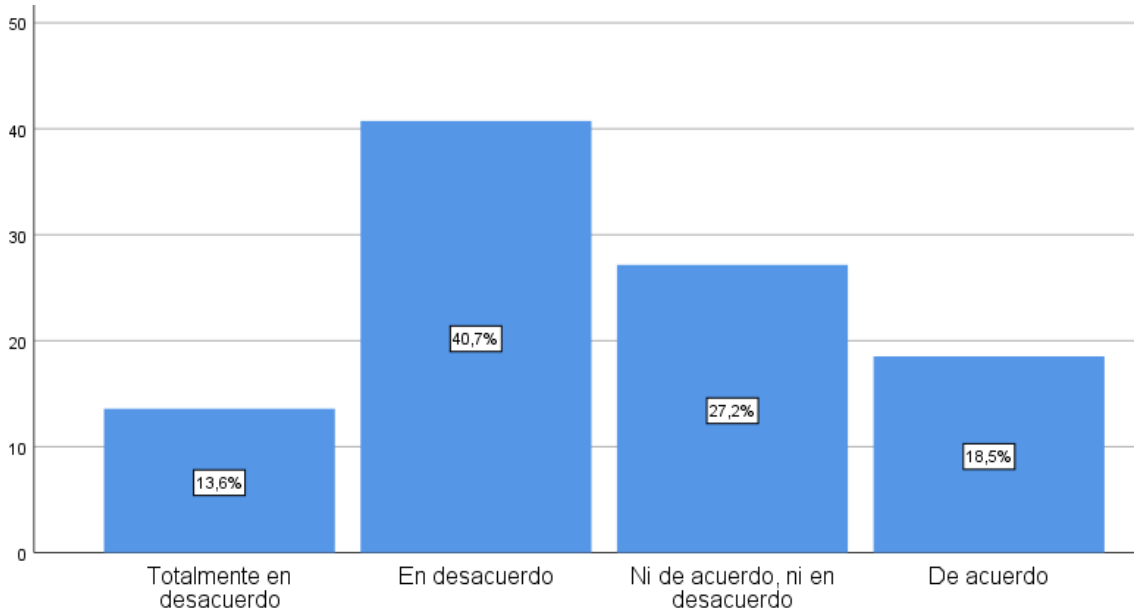


Nota: Procesado en SPSS V 26.00

Con un 32.10% de neutralidad sobre la solidez del marco legal, se observa una percepción incierta sobre la capacidad de la normativa para hacer frente a las constantes evoluciones en el ámbito del fraude informático. Este dato puede reflejar una falta de confianza en que el marco actual pueda adaptarse a la velocidad de los cambios tecnológicos, lo cual pone de manifiesto la necesidad de considerar revisiones continuas que aseguren su vigencia y pertinencia frente a las técnicas avanzadas en delitos cibernéticos.

Figura 18

¿Considera que las políticas normativas actuales fomentan adecuadamente la adopción de tecnologías de la información y comunicación para prevenir el fraude informático?

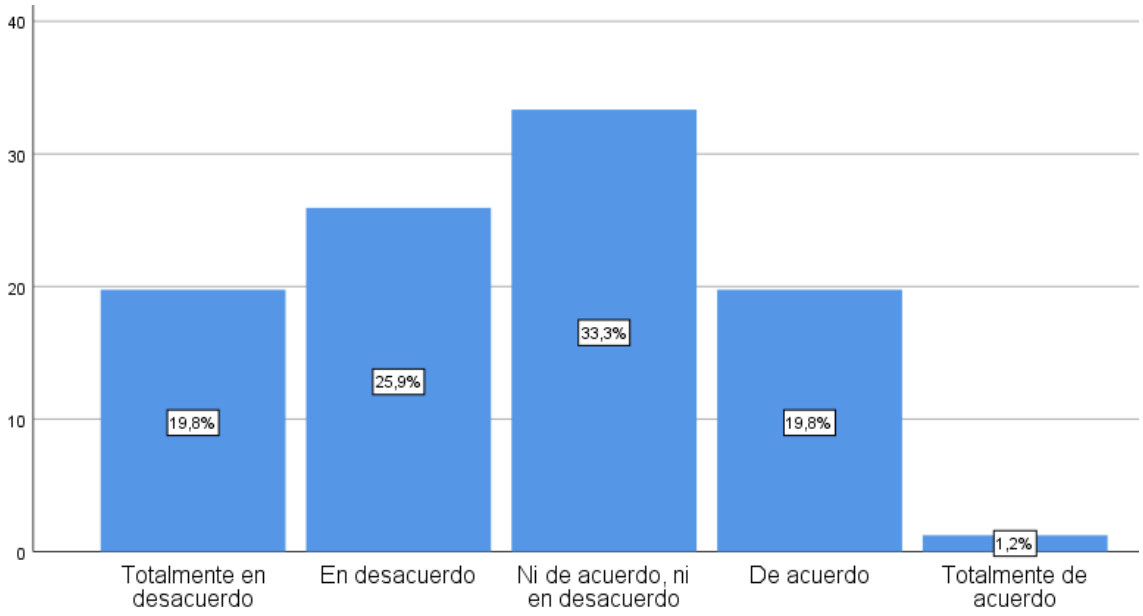


Nota: Procesado en SPSS V 26.00

Un desacuerdo del 40.70% sobre la promoción de tecnologías de prevención en la normativa vigente señala una percepción de que las leyes no están impulsando adecuadamente la adopción de soluciones tecnológicas en el combate contra los delitos digitales. Este valor refleja una brecha en la implementación de políticas que incentiven o faciliten el uso de innovaciones digitales, lo que podría estar limitando el alcance de las normativas para contrarrestar las amenazas en el entorno informático actual.

Figura 19

¿Cree que los marcos regulatorios vigentes son efectivos para garantizar una seguridad informática robusta frente a las amenazas del fraude digital?

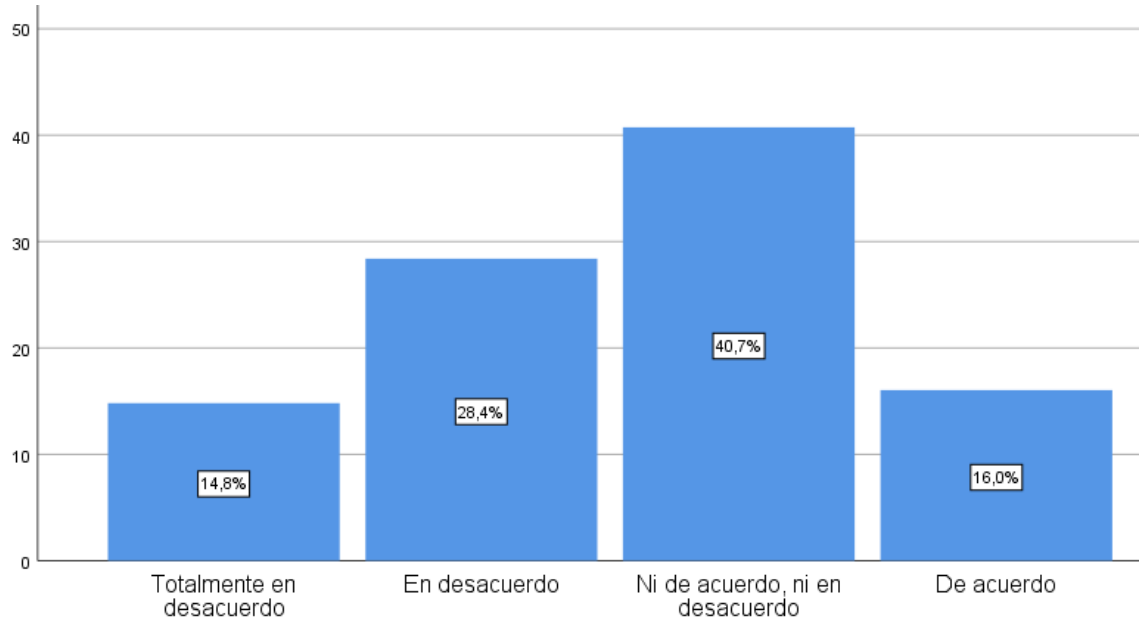


Nota: Procesado en SPSS V 26.00

Un 33.30% de respuestas neutrales respecto a la efectividad de los marcos regulatorios vigentes para garantizar seguridad informática revela una percepción de insuficiencia en los esquemas de protección actuales. Esta postura sugiere que, a pesar de la existencia de normativas, estas no logran proyectar una imagen de robustez que asegure a la ciudadanía frente a posibles fraudes, lo que podría indicar una falta de adaptabilidad o efectividad de las normativas en el contexto de amenazas digitales.

Figura 20

¿Opina que la legislación en materia de tecnología de la información y comunicación está alineada con las necesidades tecnológicas modernas para combatir el fraude cibernético?

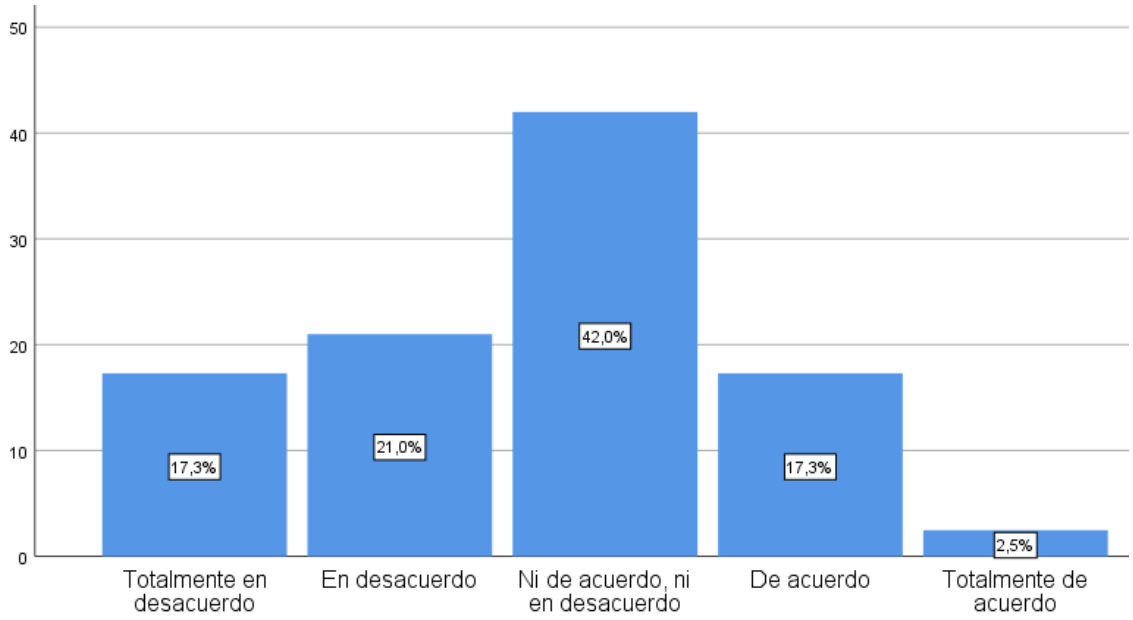


Nota: Procesado en SPSS V 26.00

Con un 40.70% de neutralidad en cuanto a la alineación de la legislación con necesidades tecnológicas, se percibe una ambigüedad en la adecuación de las normativas actuales a los avances técnicos modernos. Esta posición podría indicar que, aunque las leyes están presentes, no logran adaptarse al ritmo de los cambios, limitando su eficacia en la prevención de fraudes. Este hallazgo subraya la importancia de contar con marcos normativos que evolucionen de manera acorde a los desarrollos en tecnología de información.

Figura 21

¿Juzga que las medidas de seguridad informática establecidas en las normativas actuales son suficientes para proteger los datos sensibles contra el fraude?

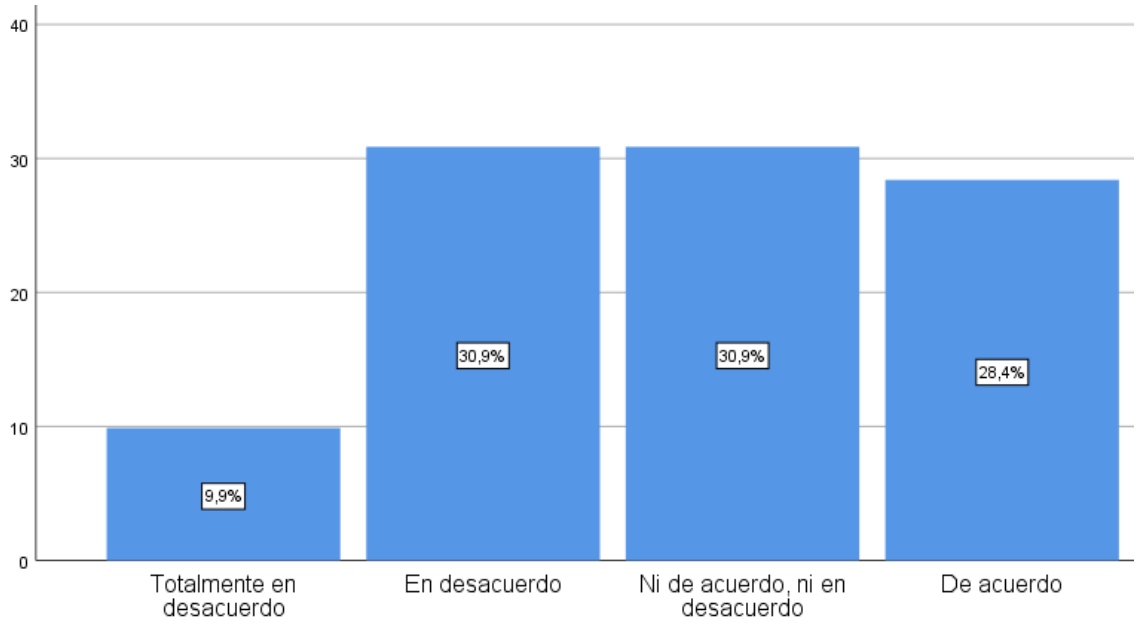


Nota: Procesado en SPSS V 26.00

Un 42.00% de respuestas neutrales en cuanto a la suficiencia de las medidas de seguridad en la normativa actual refleja una percepción incierta en cuanto a la efectividad de estas medidas para resguardar datos sensibles. La falta de un posicionamiento claro sugiere que los mecanismos vigentes no han alcanzado un nivel de aceptación generalizado, lo que podría señalar una necesidad de mejoras en las disposiciones para asegurar una protección integral frente a los riesgos informáticos.

Figura 22

¿Estima que las iniciativas gubernamentales han sido efectivas en promover la integración de tecnologías avanzadas en la lucha contra el fraude informático?

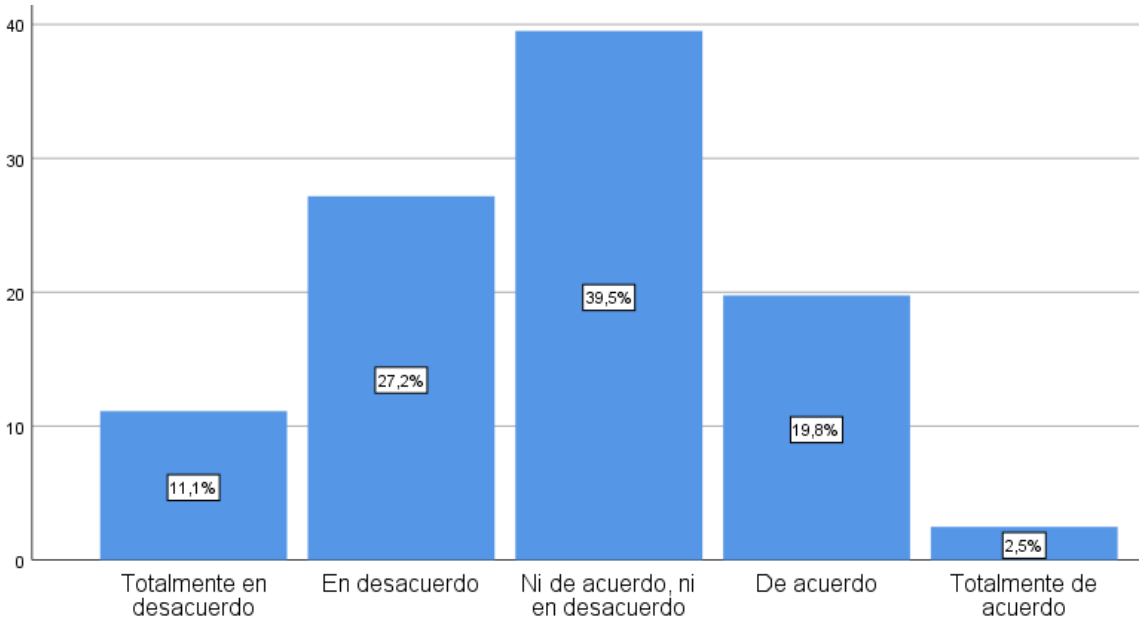


Nota: Procesado en SPSS V 26.00

Con un 30.90% de neutralidad respecto a la efectividad de las iniciativas para integrar tecnología avanzada en la prevención de fraudes, se identifica una postura ambigua sobre la capacidad de los esfuerzos actuales para incorporar innovaciones en esta área. Este valor indica que, aunque existen iniciativas, estas no están alcanzando el impacto esperado en el combate contra delitos informáticos, lo cual podría señalar una insuficiencia en los recursos asignados o en el desarrollo de políticas que incentiven dicha integración.

Figura 23

¿Considera que el marco regulatorio actual es suficiente para abordar eficazmente las diversas formas de fraude informático que afectan al país?

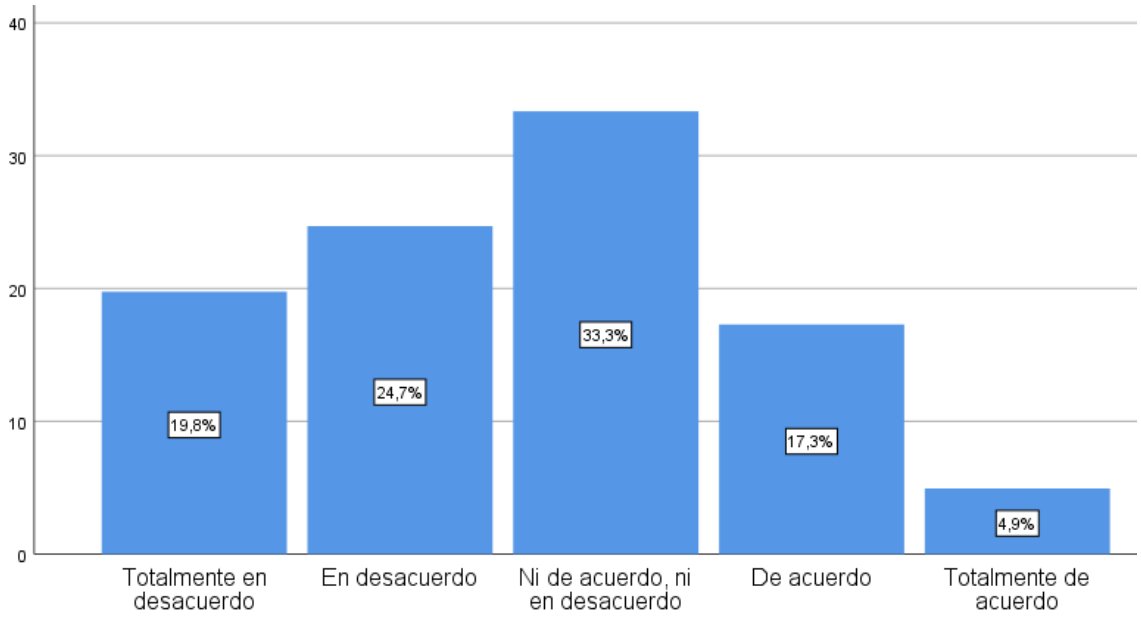


Nota: Procesado en SPSS V 26.00

Un 39.50% de neutralidad sobre la suficiencia del marco regulatorio para enfrentar diversas modalidades de fraude sugiere que las leyes actuales no logran responder adecuadamente a las múltiples facetas de estos delitos. Esta percepción podría reflejar una falta de adaptabilidad en las normativas, lo cual afecta su capacidad de disuasión y prevención frente a un entorno de delitos en constante transformación y evolución.

Figura 24

¿Cree que la aplicación de las normativas vigentes ha sido adecuada para prevenir y sancionar de manera efectiva los delitos informáticos?

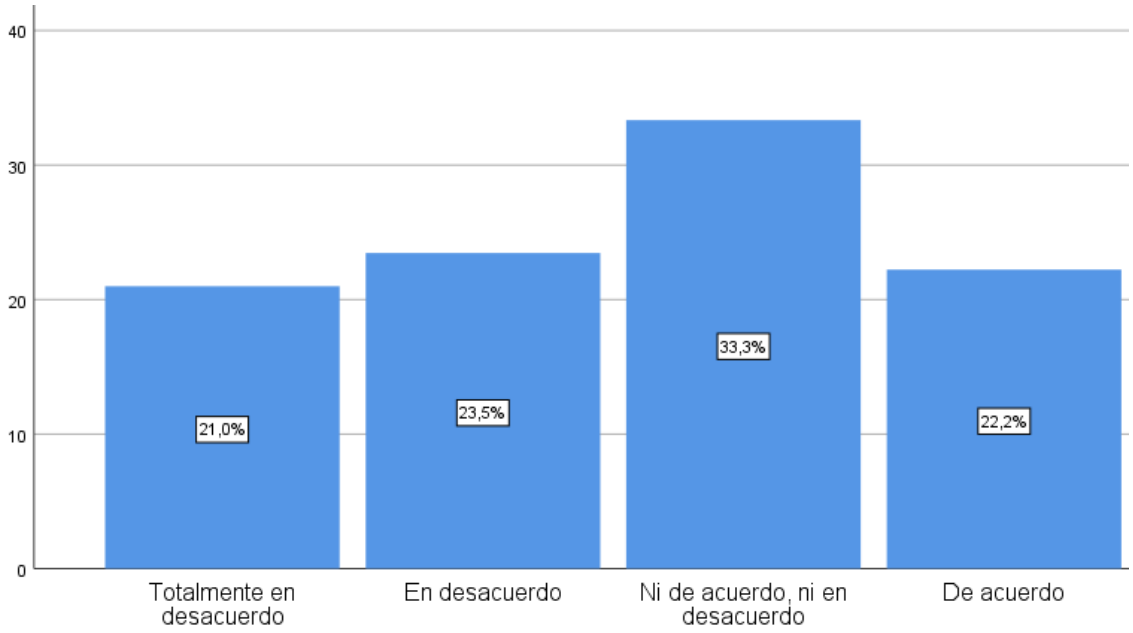


Nota: Procesado en SPSS V 26.00

El 33.30% de neutralidad respecto a la adecuación de las normativas para prevenir y sancionar delitos cibernéticos refleja una percepción de ineficacia o insuficiencia en las disposiciones actuales. Este valor indica que, si bien existen normativas, su aplicación no parece efectiva para garantizar una prevención o sanción adecuada, lo cual podría sugerir la necesidad de revisiones en los mecanismos de cumplimiento y sanción.

Figura 25

¿Opina que las leyes existentes necesitan actualizaciones para mantenerse al día con los rápidos avances tecnológicos que facilitan el fraude informático?

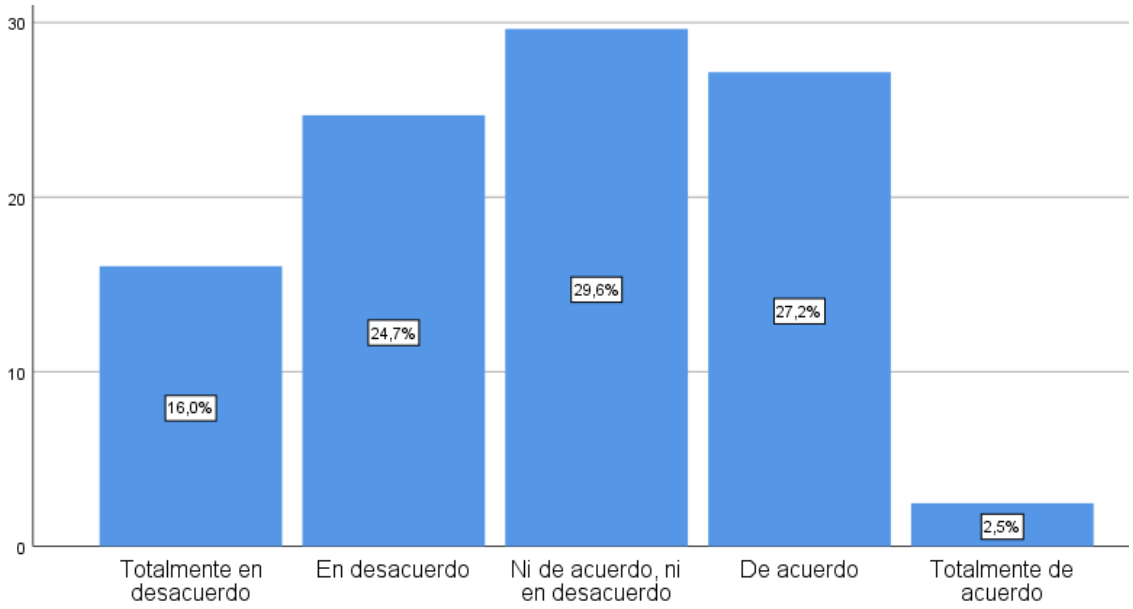


Nota: Procesado en SPSS V 26.00

Con un 33.30% de neutralidad en cuanto a la actualización de las leyes frente a los avances tecnológicos, se percibe una postura ambigua sobre la capacidad de las normativas para mantenerse vigentes en el entorno cambiante de la tecnología. Esta posición podría sugerir que, aunque las leyes están en vigor, no logran adaptarse a los cambios rápidos, lo que limita su efectividad en la prevención de fraudes sofisticados.

Figura 26

¿Juzga que las autoridades encargadas de la implementación y aplicación de las leyes contra el fraude informático están cumpliendo con sus responsabilidades de manera efectiva?

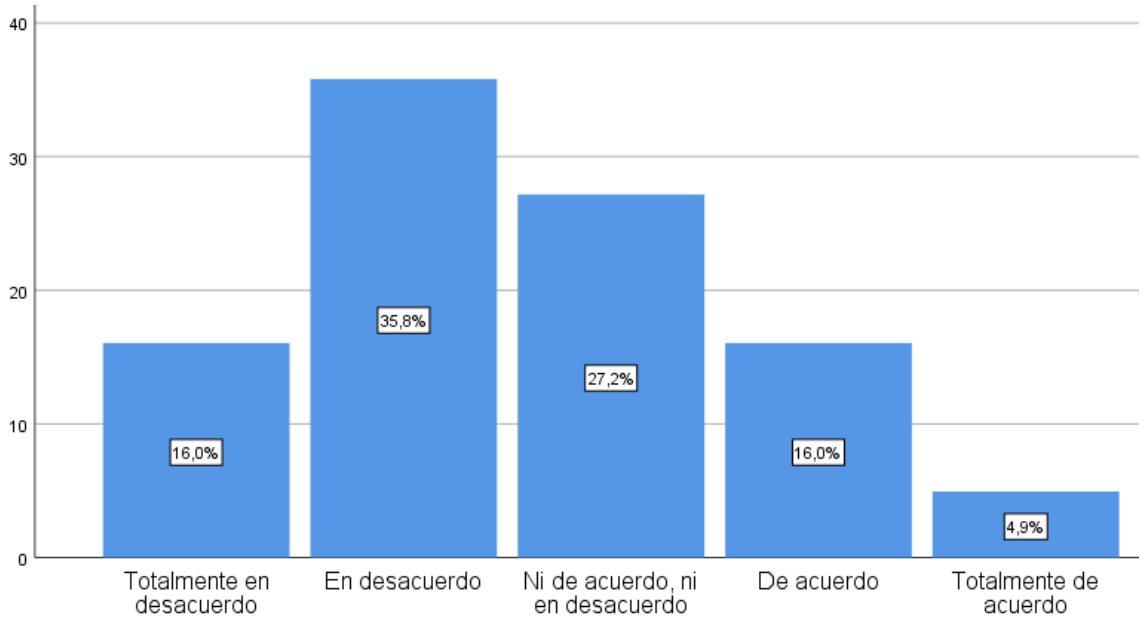


Nota: Procesado en SPSS V 26.00

La neutralidad del 29.60% sobre la efectividad en el cumplimiento de responsabilidades de las autoridades encargadas indica una percepción de poca confianza en su desempeño en la implementación de normativas. Este valor sugiere que, aunque existen organismos responsables, su gestión no logra transmitir una imagen de eficiencia, lo que podría estar asociado con una percepción de insuficiencia en recursos o en la formación necesaria para el cumplimiento de sus deberes.

Figura 27

¿Estima que el tratamiento normativo dado al fraude informático es suficientemente exhaustivo para cubrir todas las posibles brechas de seguridad cibernética?

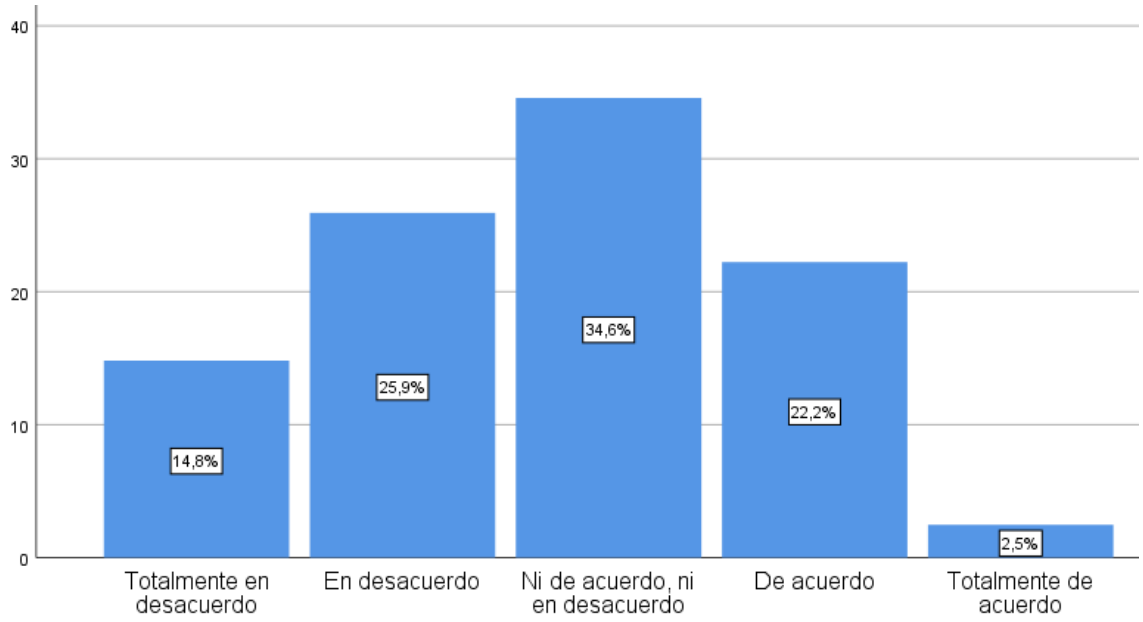


Nota: Procesado en SPSS V 26.00

Un desacuerdo del 35.80% sobre la exhaustividad en el tratamiento normativo sugiere que las leyes actuales no cubren todas las posibles brechas de seguridad. Esta percepción podría estar relacionada con la falta de disposiciones específicas que aborden diferentes formas de ataques en el entorno digital, evidenciando una necesidad de fortalecer la normativa para abarcar las vulnerabilidades emergentes y reducir así la exposición al riesgo.

Figura 28

¿Considera que las normativas actuales contemplan adecuadamente la diversidad de tipos de fraude informático que existen en el entorno digital?

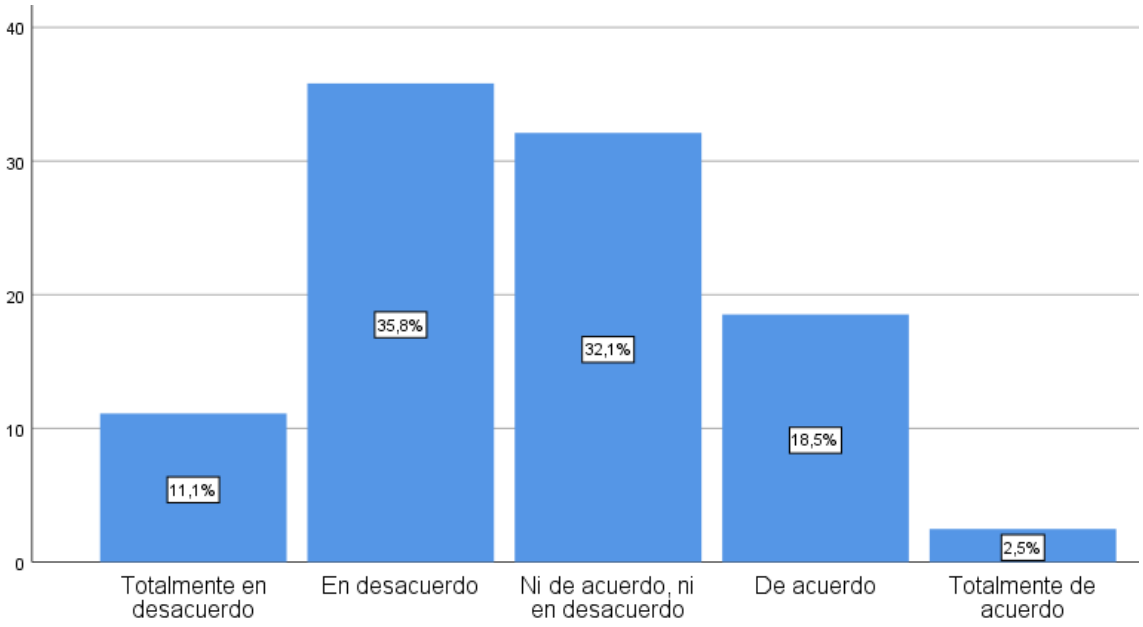


Nota: Procesado en SPSS V 26.00

Con un 34.60% de neutralidad sobre la contemplación de los tipos de fraude existentes, se percibe una postura ambigua respecto a la amplitud de la normativa actual. Este resultado podría sugerir que la legislación no está abordando de manera adecuada la diversidad de formas que adquiere el fraude en el ámbito digital, lo que señala una necesidad de revisar el alcance de la ley para mejorar su aplicabilidad en contextos específicos.

Figura 29

¿Cree que las estrategias normativas vigentes son efectivas para contrarrestar los métodos de ataque informático más sofisticados y en constante evolución?

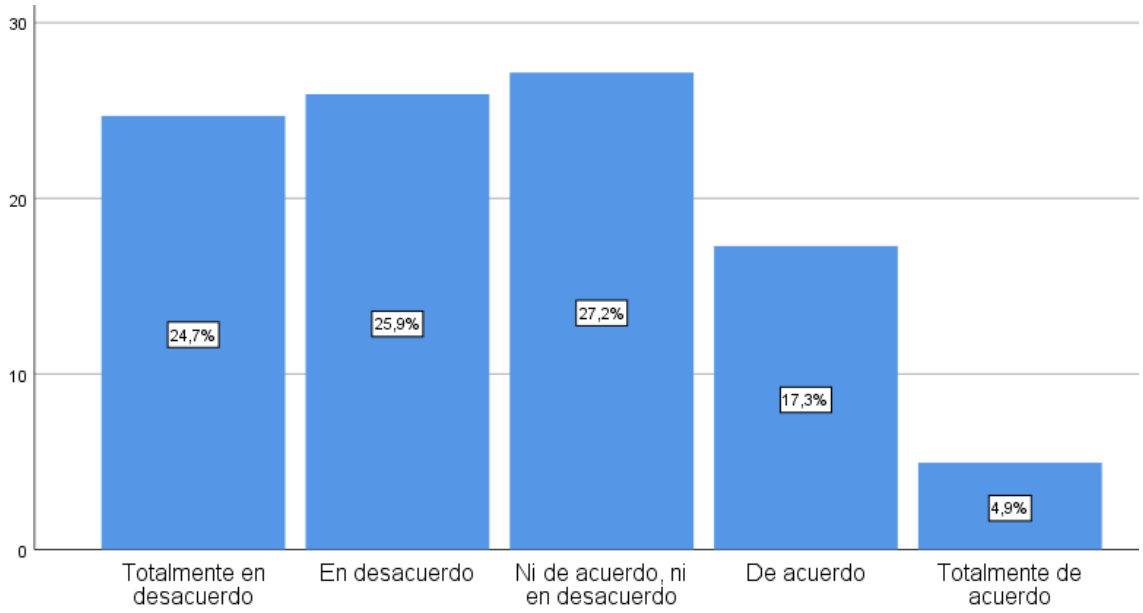


Nota: Procesado en SPSS V 26.00

El 35.80% en desacuerdo sobre la eficacia de las estrategias normativas contra ataques sofisticados indica una percepción de ineficacia en los mecanismos actuales. Este valor podría reflejar una insuficiencia en la adaptabilidad de las normativas frente a las nuevas modalidades de fraude, lo que sugiere una necesidad de fortalecimiento en las estrategias legislativas para garantizar una mayor protección frente a amenazas tecnológicas avanzadas.

Figura 30

¿Opina que las legislaciones actuales abordan de manera integral las diferentes modalidades de fraude cibernético que afectan a los usuarios y a las empresas?

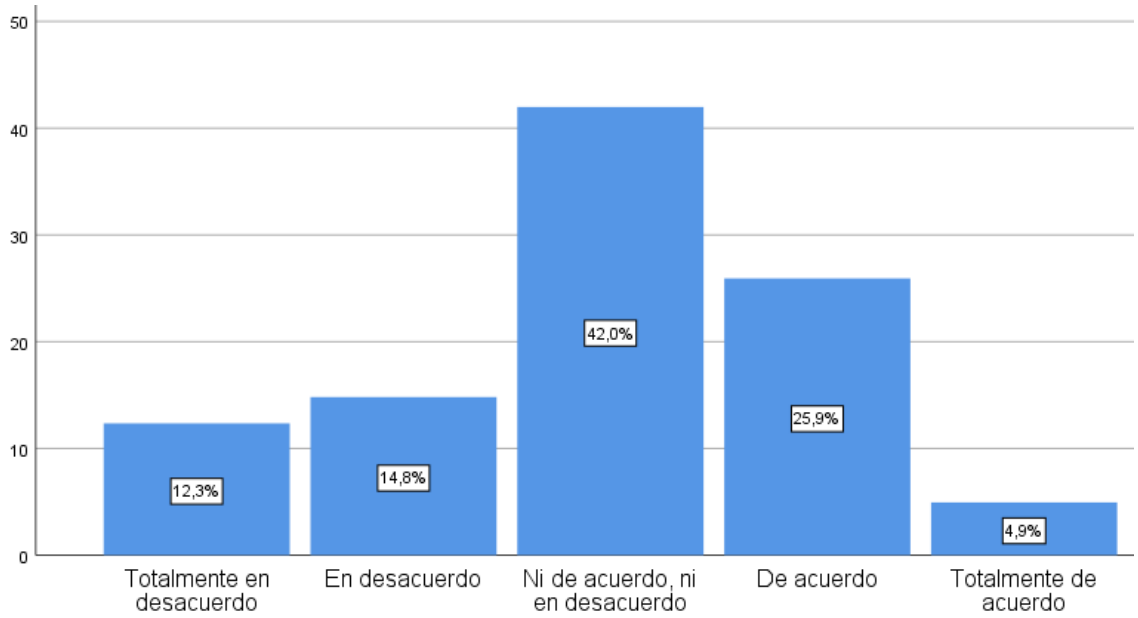


Nota: Procesado en SPSS V 26.00

Un 27.20% de neutralidad sobre la integralidad de las legislaciones en la protección contra fraudes digitales sugiere una percepción ambigua respecto a la capacidad de la normativa para abarcar las distintas modalidades de fraude. Esta postura podría indicar que, aunque existen disposiciones, estas no logran cubrir las necesidades de protección en todos los contextos, lo que puede señalar áreas de oportunidad en la normativa para asegurar una cobertura más amplia.

Figura 31

¿Juzga que las autoridades han implementado medidas adecuadas para prevenir y responder a los métodos de ataque informático emergentes?

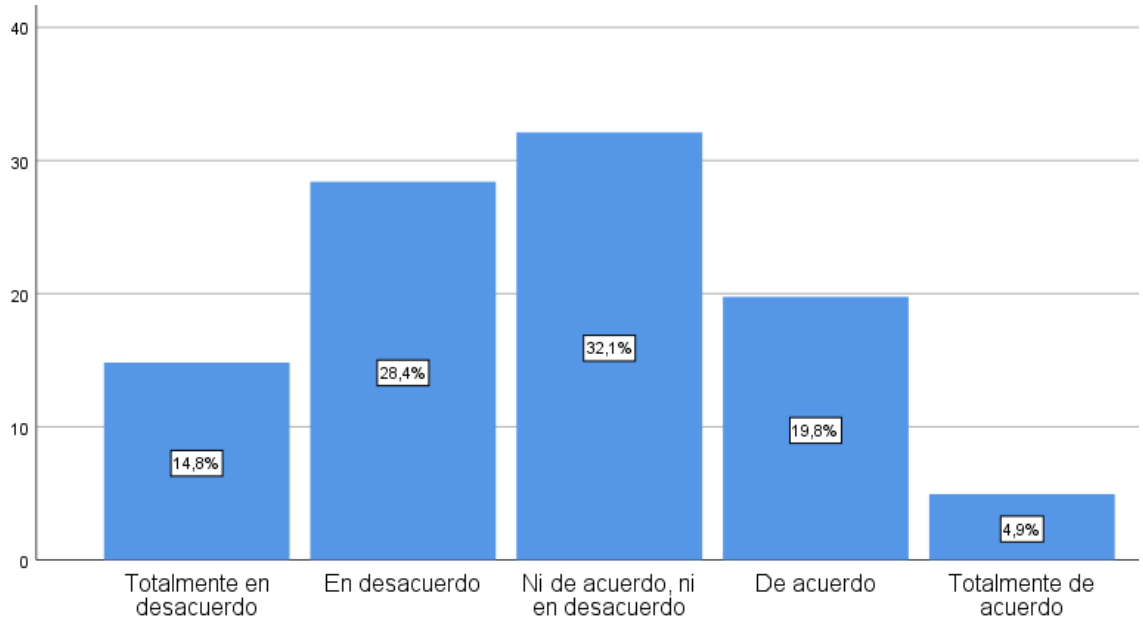


Nota: Procesado en SPSS V 26.00

Con un 42.00% de respuestas neutrales en cuanto a las medidas preventivas frente a ataques emergentes, se percibe una incertidumbre sobre la capacidad de la normativa para adaptarse a nuevas amenazas. Este valor refleja una posible falta de actualización en las estrategias de prevención y respuesta, lo que limita la percepción de seguridad y podría estar relacionado con una insuficiencia en la efectividad de los mecanismos vigentes.

Figura 32

¿Estima que las políticas públicas en vigor están suficientemente preparadas para hacer frente a las nuevas variantes de fraude informático que surgen con el avance de la tecnología?



Nota: Procesado en SPSS V 26.00

Un 32.10% de neutralidad sobre la preparación de las políticas frente a variantes avanzadas de fraude señala una percepción de insuficiencia en la adaptación de las normativas a los avances tecnológicos. Este valor refleja una posible brecha en la capacidad de la normativa para responder a nuevas formas de fraude, lo que podría sugerir una necesidad de fortalecer los aspectos de actualización continua y mejorar la preparación para enfrentar el cambio tecnológico en el ámbito regulatorio.

Estadística inferencial

Prueba de normalidad

Tabla 2

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Tratamiento político – normativo	,361	81	,000	,696	81	,000
Fraude informático	,350	81	,000	,725	81	,000

Nota: Procesado en el software SPSS V 26.00

Empleando un grupo de estudio que supera los 50 individuos, se validó el índice Kolmogorov-Smirnov, registrando una sigma inferior a 0.050, lo que confirmó una dispersión no paramétrica. Posteriormente, se utilizó el coeficiente Rho de Spearman para evidenciar la relación entre los factores analizados.

Objetivo General

Tabla 3

Correlación entre la variable Tratamiento político - normativo y la variable Fraude informático

		Fraude informático
Tratamiento político - normativo	Relación Rho de Spearman	0.788
	Sigma	0.000
	N	81

Nota: Procesado en el software SPSS V 26.00

Se logró una validación estadística con un nivel de significancia inferior a 0.050, evidenciando un índice de relación de 0.788. Esto indica una vinculación muy fuerte y directamente proporcional entre los elementos comparados.

Objetivo específico 1

Tabla 4

Correlación entre la dimensión Ley N° 30096 y la variable Fraude informático

		Fraude informático
Ley N° 30096	Relación Rho de Spearman	0.691
	Sigma	0.000
	N	81

Nota: Procesado en el software SPSS V 26.00

Se logró una validación estadística con un nivel de significancia inferior a 0.050, evidenciando un índice de relación de 0.691. Esto indica una vinculación considerable y directamente proporcional entre los elementos comparados.

Objetivo específico 2

Tabla 5

Correlación entre la dimensión Delito informático y la variable Fraude informático

		Fraude informático
Delito informático	Relación Rho de Spearman	0.731
	Sigma	0.000
	N	81

Nota: Procesado en el software SPSS V 26.00

Se logró una validación estadística con un nivel de significancia inferior a 0.050, evidenciando un índice de relación de 0.731. Esto indica una vinculación considerable y directamente proporcional entre los elementos comparados.

Objetivo específico 3

Tabla 6

Correlación entre la dimensión Tecnología de la información y comunicación, y la variable Fraude informático

		Fraude informático
Tecnología de la información y comunicación	Relación Rho de Spearman	0.779
	Sigma	0.000
	N	81

Nota: Procesado en el software SPSS V 26.00

Se logró una validación estadística con un nivel de significancia inferior a 0.050, evidenciando un índice de relación de 0.779. Esto indica una vinculación muy fuerte y directamente proporcional entre los elementos comparados.

IV. Discusión

El análisis del **objetivo general,** en cuanto al tratamiento político normativo evidencia una correlación de 0.788 en la relación entre las políticas regulatorias y la frecuencia del fraude informático en el contexto peruano. Esta relación destaca que el establecimiento de límites y sanciones concretas es esencial para incrementar la seguridad y robustez de los sistemas digitales y, de este modo, elevar la confianza en el uso de plataformas electrónicas.

A diferencia del enfoque metodológico de los estudios previos, Calva y Nivelo (2021) observaron en sus investigaciones que el adecuado manejo de los delitos informáticos demanda una constante capacitación y mejoras estructurales en el sistema judicial, especialmente en los procesos de juzgamiento. La falta de conocimiento especializado entre operadores de justicia se evidenció como un obstáculo significativo, subrayando una carencia de recursos que afecta directamente la persecución y sanción de estos crímenes. En este sentido, el estudio destaca que el desconocimiento sobre el procesamiento de delitos informáticos limita el avance en sanciones efectivas, un aspecto crucial para establecer una respuesta robusta ante tales delitos. El resultado arrojó un 0.788 en la relación entre las normativas y el fraude en el contexto fiscal peruano, revelando un contraste en el desarrollo de políticas enfocadas en la prevención y contención del fraude digital, al sugerir que un tratamiento más sólido puede mejorar el control de los delitos en entornos virtuales. Por otra parte, Díaz (2023) destacó la necesidad de un cambio de enfoque en los operadores judiciales y del sector financiero, quienes requieren de una mayor capacitación para enfrentar los delitos cibernéticos. El estudio enfatiza una perspectiva de adecuación y adaptación legislativa en un entorno de ciberseguridad que exige esfuerzos constantes, encontrando que la falta de estrategias nacionales bien implementadas obstaculiza la prevención de fraudes. Al compararse con los avances obtenidos en el análisis peruano, donde la normatividad ha incorporado lineamientos para sancionar prácticas de manipulación y abuso informático, se observa una diferencia en la actualización de medidas regulatorias, ya que el autor concluye que la legislación actual en Ecuador no ha logrado adaptarse plenamente a la evolución de los delitos digitales. La referencia numérica al 2023 en el contexto ecuatoriano también sugiere una dinámica normativa que se encuentra en constante cambio, aunque los resultados no garantizan una mejora suficiente para reducir significativamente el impacto del fraude cibernético en el sector financiero.

Desde una perspectiva crítica, el enfoque de la normativa que aborda los delitos informáticos suele requerir una estructura de regulación flexible que se adapte a los constantes avances tecnológicos. El aumento en la frecuencia y complejidad de los fraudes en plataformas digitales exige la creación de estrategias jurídicas y técnicas altamente específicas, dirigidas no solo a la contención, sino también a la prevención de actividades ilícitas en línea. Así, los sistemas de protección se configuran alrededor de

un marco que facilite la identificación temprana de vulnerabilidades y respalde la colaboración entre instituciones nacionales e internacionales. Esta adaptación no se limita a la implementación de leyes, sino que involucra un desarrollo integral en los campos de la tecnología y el conocimiento especializado para todos los operadores de justicia y personal involucrado. El reto no solo reside en la imposición de sanciones, sino en un avance normativo que permita afrontar los riesgos cibernéticos de manera anticipada y articulada.

En consecuencia, el tratamiento jurídico de los delitos digitales demanda una implementación que considere tanto el ámbito legal como el educativo en las instituciones encargadas de la justicia. Al respecto, Cuellar y Astaiza (2024) han señalado que las políticas de regulación efectiva deben configurarse como una respuesta preventiva que anticipe los cambios en los mecanismos de fraude y que incluya la supervisión constante de infraestructuras digitales. Asimismo, Tacuche (2023) enfatiza que una política jurídica sólida requiere de la actualización continua en las normas y estrategias de monitoreo, adaptándose a los desafíos tecnológicos con base en una infraestructura digital segura. A su vez, estos estudios refuerzan que una adaptación legislativa eficaz no solo se basa en la regulación estricta, sino en una proyección preventiva que, al integrar tecnologías emergentes, mantenga la integridad de las transacciones digitales y reduzca los riesgos de fraude cibernético.

En cuanto al **objetivo específico 1,** el análisis de la Ley N° 30096 establece una correlación de 0.691 con la prevención de fraudes informáticos, reflejando un enfoque de control preventivo y sancionador que contribuye a la seguridad digital. Esta ley proporciona un marco normativo riguroso, promoviendo una protección efectiva contra el acceso indebido a sistemas, lo cual favorece un entorno virtual más seguro y confiable.

Inicialmente, Cuellar y Astaiza (2024) realizaron un análisis exhaustivo de la legislación colombiana en torno a delitos de fraude informático, destacando la necesidad de contar con regulaciones penales específicas y efectivas. Se mostró que la legislación penal en Colombia ha facilitado la intervención de las autoridades para manejar de manera eficiente los delitos informáticos, un factor que se relaciona de manera contrastante con los resultados obtenidos bajo la Ley N° 30096. Al enfocar sus esfuerzos en el refuerzo normativo y en la protección del desarrollo digital, los autores reflejan la efectividad de políticas que abarcan un amplio espectro de prácticas de seguridad. Sin embargo, en comparación con la Ley N° 30096, que ha establecido una relación de 0.691 con el fraude informático, los hallazgos en Colombia sugieren una mayor eficacia en cuanto a la ejecución de sanciones. En efecto, el análisis colombiano recalca el papel de una legislación adaptada a los desafíos tecnológicos, promoviendo no solo la contención, sino también un nivel de protección integral en el ámbito digital, lo cual sugiere que se requeriría una mayor alineación normativa para alcanzar niveles óptimos de prevención en otros contextos. Por otro lado, Delgado (2022) enfoca su estudio en la deficiencia del tratamiento penal de los

delitos informáticos, especialmente en el contexto de protección patrimonial. Según su análisis, el 70% de los participantes percibieron un aumento en los delitos informáticos debido al desarrollo de las tecnologías de la información, señalando que la falta de medidas preventivas de las entidades bancarias también agrava esta problemática. En comparación, los resultados peruanos bajo la Ley N° 30096 muestran un enfoque normativo que regula el uso de sistemas electrónicos para una detección oportuna de prácticas ilícitas, un aspecto que contrasta con el estudio al sugerir una aplicación limitada de la ley en el contexto penal de Chimbote. La legislación peruana, en este sentido, parece estar diseñada con mayor rigor en cuanto a la regulación del acceso indebido a sistemas digitales, abordando de manera más puntual los delitos cibernéticos. Sin embargo, el análisis enfatiza que en muchos casos no se han implementado medidas adecuadas para prevenir el fraude en entornos bancarios, reflejando así una falta de consistencia en la eficacia del tratamiento penal en su entorno local.

En el ámbito normativo que se ocupa de los delitos cibernéticos, se observa que la adaptación de políticas a las particularidades de los sistemas digitales es fundamental para enfrentar el fraude de manera efectiva. Los marcos legales eficaces buscan no solo sancionar las infracciones una vez ocurridas, sino anticipar el comportamiento criminal mediante disposiciones preventivas y estrategias de control. En este sentido, el marco jurídico juega un rol central en la implementación de procedimientos que garanticen la seguridad del entorno digital y la protección de los datos, permitiendo un espacio de actuación donde las instituciones públicas y privadas pueden operar con confianza. Además, el avance tecnológico constante demanda que las normativas se actualicen regularmente, de manera que se mantengan alineadas con las amenazas emergentes. Sin estas actualizaciones y un enfoque integral, la normativa podría convertirse en un recurso insuficiente para la prevención y control de fraudes, especialmente en áreas de alta vulnerabilidad como las plataformas financieras y comerciales.

Consecuentemente, el tratamiento de delitos informáticos bajo una normativa específica ofrece un mecanismo crucial de control y protección ante conductas ilícitas. En efecto, Alcántara (2024) ha señalado que las normativas para combatir fraudes deben incluir tanto medidas sancionadoras como procedimientos técnicos para identificar y mitigar estos delitos en sus fases tempranas. Asimismo, Ramos y Salvador (2022) concluyeron que una política legislativa eficaz debe integrar la actualización constante de las leyes, permitiendo así que el marco legal se mantenga robusto frente a las amenazas que surgen con el desarrollo de nuevas tecnologías. En este sentido, su investigación plantea que la normativa eficaz es aquella que se anticipa a los métodos de fraude y cuenta con disposiciones que fortalecen la infraestructura de seguridad digital. La integración de estos conceptos en las políticas contra el fraude informático permite crear un marco regulador adaptado a los desafíos de un entorno en permanente transformación, reduciendo la vulnerabilidad de las instituciones.

En referencia con el **objetivo específico 2,** el estudio de la relación de los delitos informáticos muestra una correlación de 0.731 con el fraude digital, subrayando que la especificación detallada de cada infracción en los lineamientos es esencial para mejorar el control y sanción de estos delitos. Esta normativa refuerza la seguridad del entorno virtual al ofrecer una respuesta jurídica eficaz frente a la comisión de delitos cibernéticos.

En comparación, Ramos y Salvador (2022) exploraron los patrones de fraude digital en Huaraz, enfocándose en modalidades como el "smishing", una técnica prevalente entre la ciudadanía debido al uso extendido de aplicaciones de mensajería que facilitan estas prácticas ilícitas. Aunque el análisis identifica un número significativo de incidentes que involucran el acceso no autorizado a datos personales, los autores revelan que la ausencia de actualizaciones normativas limita la capacidad del sistema legal para responder adecuadamente a tales modalidades emergentes. Esto contrasta con el marco analizado, en el cual la correlación de 0.731 resalta la importancia de lineamientos detallados para clasificar y sancionar adecuadamente las infracciones digitales. La incorporación de categorías específicas para cada práctica podría no solo fortalecer el entorno jurídico, sino también reducir el espacio de maniobra de estas prácticas en rápida evolución. En consecuencia, mientras que en el contexto estudiado por Ramos y Salvador se plantea la necesidad de mejoras específicas en la Ley N° 3009, el análisis peruano sugiere que una regulación más completa que abarque la tipificación de cada acción ilícita es esencial para un control efectivo de los delitos informáticos. Asimismo, Alcántara (2024) subrayó en su estudio sobre la Ley N° 30096 la existencia de vacíos legales que impiden una sanción eficaz contra el fraude en plataformas digitales, siendo estos vacíos legales señalados por el 60% de los expertos consultados en su investigación. La aplicación actual de la ley, según los resultados de Alcántara, muestra una dificultad en garantizar una respuesta adecuada debido a la insuficiencia de especialistas en el manejo de delitos digitales, situación que contribuye a la vulnerabilidad de los sistemas informáticos. En comparación, el análisis bajo la dimensión del delito informático evidencia que la precisión en los lineamientos y la correcta clasificación de infracciones digitales puede generar un impacto positivo en la reducción del fraude digital, alcanzando una relación de 0.731. Esta cifra indica que un marco más exhaustivo y técnicamente orientado, en contraposición con las deficiencias observadas por el autor en la legislación evaluada, permitiría alcanzar un ambiente cibernético más seguro. El estudio concluye que el perfeccionamiento del marco legal en torno a los delitos informáticos resulta crucial para lograr un mayor grado de eficacia en la protección de la infraestructura digital.

El abordaje jurídico de las infracciones digitales requiere una constante actualización normativa que considere la naturaleza dinámica de las amenazas digitales. A diferencia de otros tipos de delitos, los crímenes en el entorno cibernético evolucionan rápidamente, y las herramientas legales necesitan abarcar sus múltiples formas y mecanismos de ejecución. En este contexto, un marco normativo que

priorice la especificación de las modalidades de los delitos informáticos resulta fundamental para asegurar una respuesta ajustada a las características particulares de cada infracción. La construcción de normativas que incluyan medidas técnicas y sanciones apropiadas permite una mayor capacidad de reacción en los operadores de justicia y, en consecuencia, un fortalecimiento de la seguridad en el ecosistema digital. A su vez, la adecuada tipificación de cada acción ilícita en el ámbito virtual contribuye a limitar la impunidad, al facilitar la identificación y el procesamiento judicial de quienes actúan al margen de la ley en entornos digitales, manteniendo un espacio más seguro para los usuarios.

En consecuencia, el tratamiento de delitos informáticos exige lineamientos precisos que permitan su identificación y sanción de forma efectiva. Por otra parte, Delgado (2022) indican que la normativa en delitos informáticos debe considerar la inclusión de categorías específicas para cada modalidad, permitiendo una mayor claridad en el procesamiento judicial. A su vez, Cuellar y Astaiza (2024) argumentan que los delitos en el entorno digital requieren de un marco que se adapte a la naturaleza cambiante de las infracciones cibernéticas, promoviendo un entorno que respalde la seguridad informática a nivel institucional y ciudadano. Este enfoque permite que la normativa esté en constante revisión, incrementando así su capacidad para combatir las infracciones en el ámbito digital. La implementación de una estructura legal robusta reduce las brechas en el control de delitos informáticos, permitiendo así que las plataformas digitales operen en un ambiente de mayor seguridad y prevención.

La investigación en cuanto al **objetivo específico 3** determina una correlación de 0.779 entre las tecnologías de información y comunicación y la prevención del fraude digital. Estas tecnologías permiten un control reforzado en entornos virtuales, promoviendo la seguridad y evitando actos de manipulación indebida mediante sistemas que protegen la integridad y confidencialidad de la información.

Por otra parte, Tacuche (2023) investigó el impacto de los actos de investigación en el tratamiento normativo de los fraudes informáticos y concluyó que las diligencias preliminares frecuentemente no son suficientes para identificar a los responsables. Esta insuficiencia destaca una problemática central: la ausencia de medidas estructuradas que permitan una mayor efectividad en la identificación y sanción de los infractores. En este sentido, la investigación difiere del análisis peruano, que apunta a una correlación de 0.779, subrayando la importancia de una infraestructura tecnológica robusta en la prevención del fraude digital. La investigación peruana sugiere que contar con sistemas de alta seguridad es clave para limitar el acceso no autorizado y la manipulación de información en entornos digitales. Aunque se resalta la necesidad de capacitación para los investigadores, la evidencia peruana resalta que el diseño de sistemas con capacidades de control y prevención podría ser una estrategia preventiva que complemente los actos de investigación. Así, se observa que el desarrollo de tecnología de avanzada y la capacitación del personal operativo pueden actuar como pilares para mejorar el control de fraudes

digitales. Asimismo, Calva y Nivelo (2021) examinaron el tratamiento de los delitos informáticos, destacando que el éxito en el manejo de estos casos depende de la capacitación constante de operadores judiciales y de una infraestructura tecnológica adecuada, aspectos señalados como prioritarios por el 70% de los operadores de justicia en su investigación. Esta necesidad de formación coincide en parte con los enfoques peruanos, que buscan reforzar la infraestructura tecnológica para contrarrestar los riesgos de manipulación de información. Sin embargo, el estudio peruano enfatiza el valor de los sistemas tecnológicos avanzados y de su rol preventivo para asegurar la confidencialidad de los datos. Por el contrario, los autores sugieren que la falta de preparación técnica en los operadores judiciales y la escasez de convenios internacionales dificultan la lucha contra la ciberdelincuencia. Este contraste subraya que, mientras en Perú se prioriza la inversión en tecnología para la prevención de fraudes digitales, la realidad ecuatoriana demanda un fortalecimiento de capacidades humanas y colaboraciones transnacionales para abordar estos delitos de manera integral.

En el ámbito de la tecnología y su relación con la seguridad digital, es evidente que el desarrollo de infraestructuras avanzadas no solo permite la detección temprana de fraudes, sino que también genera un ambiente en el cual los datos personales se resguardan contra accesos indebidos. Las plataformas digitales, al estar en constante evolución, requieren de sistemas adaptables que prevengan actos ilícitos mediante la implementación de tecnologías de seguridad, como los sistemas de autenticación robusta y de monitoreo continuo. Estas soluciones técnicas se convierten en un recurso fundamental para mitigar las vulnerabilidades en entornos virtuales, sobre todo considerando que las amenazas en el espacio digital aumentan en frecuencia y sofisticación. Además, la integración de estos sistemas tecnológicos con políticas de formación para los operadores permite una respuesta más eficaz y estructurada ante incidentes de seguridad, optimizando tanto los procesos de detección como de intervención. Con estos recursos, es posible no solo establecer barreras para la manipulación de información, sino también reforzar el marco normativo que protege el flujo de datos en la esfera digital.

A su vez, la adecuación de infraestructuras tecnológicas frente a delitos informáticos permite fortalecer los mecanismos de protección de datos y prevenir conductas no autorizadas. Por lo tanto, Díaz (2023) señala que el desarrollo tecnológico debe incluir mecanismos de monitoreo que limiten los accesos indebidos y brinden un seguimiento eficaz. Asimismo, Calva y Nivelo (2021) recalcaron que los sistemas de seguridad digital necesitan herramientas de vigilancia activa que ayuden a identificar posibles amenazas, garantizando así una protección integral en plataformas digitales. Estos estudios indican que, para optimizar la protección en el entorno cibernético, las tecnologías deben ser no solo preventivas, sino también reactivas, capaces de adaptarse y de actualizarse según las tendencias del fraude digital. En definitiva, la integración de soluciones avanzadas y adaptativas en el ecosistema

tecnológico contribuye a mantener un ambiente digital seguro, resguardando tanto la privacidad como la integridad de la información.

V. Conclusiones

1. El tratamiento político normativo demostró una relación de 0.788 respecto al fraude informático, debido a que, las actividades ilícitas en entornos digitales representan un desafío creciente, las estrategias regulatorias incorporan lineamientos que permiten la identificación y sanción de prácticas de manipulación o engaño. Esta intervención normativa busca establecer límites claros y robustos, permitiendo una mejor protección de los datos y sistemas ante intervenciones no autorizadas, lo que refuerza la seguridad y confianza en el uso de plataformas electrónicas.

2. La Ley N° 30096 demostró una relación de 0.691 respecto al fraude informático, debido a que, la legislación actual aborda los desafíos que plantea el acceso indebido a sistemas de información, las disposiciones legales otorgan un marco detallado que estipula sanciones frente a las infracciones en el entorno digital. Este enfoque regula el uso adecuado de sistemas electrónicos y promueve mecanismos de control efectivos que permiten la detección oportuna de conductas ilícitas, contribuyendo así a un entorno de seguridad en el ámbito virtual.

3. El delito informático demostró una relación de 0.731 respecto al fraude informático, debido a que, el aprovechamiento indebido de medios electrónicos requiere de normativas que permitan su adecuada clasificación, el desarrollo de lineamientos que describan específicamente las diversas infracciones digitales es esencial. Estos lineamientos facilitan la tipificación de cada acción no autorizada, promoviendo sanciones acordes y fomentando un entorno seguro al limitar la impunidad en actos que puedan afectar el ecosistema digital y su integridad.

4. La tecnología de la información y comunicación demostró una relación de 0.779 respecto al fraude informático, debido a que, la manipulación de información a través de plataformas digitales utiliza infraestructuras de tecnología avanzada, el diseño de sistemas robustos y seguros es esencial para contrarrestar prácticas fraudulentas. La implementación de mecanismos tecnológicos adecuados fortalece el control en los entornos virtuales, permitiendo una mejor prevención de actos no autorizados y protegiendo la confidencialidad de los datos mediante la adecuada gestión de las herramientas digitales disponibles.

VI. Recomendaciones

1. En el contexto de fortalecer el combate contra el fraude informático, resulta pertinente que el Ministerio Público del Distrito Fiscal del Callao revise y optimice el marco de políticas y normas que regulan la persecución de delitos digitales. Esta revisión debe orientarse hacia la identificación de vacíos normativos o ambigüedades en el tratamiento político de los delitos informáticos que puedan dificultar la acción penal efectiva. La recomendación apunta a establecer un tratamiento normativo más riguroso, que permita una respuesta contundente ante estos delitos, a fin de prevenir el uso de brechas legales en favor de los infractores, mejorando así la capacidad del sistema para enfrentar el fraude informático de manera ágil y efectiva.

2. Es fundamental que el Ministerio Público del Distrito Fiscal del Callao realice un análisis profundo de la aplicación práctica de la Ley N° 30096 en los casos de fraude informático. La recomendación está enfocada en estudiar los criterios interpretativos y los resultados judiciales previos para identificar tanto las fortalezas como las áreas de mejora en la implementación de esta normativa. Este análisis permitirá orientar ajustes normativos y operativos que se traduzcan en una aplicación más eficaz de la ley, garantizando que su impacto sea significativo en la reducción de delitos informáticos dentro del ámbito jurisdiccional, fortaleciendo la confianza en la capacidad de las autoridades para gestionar estos casos con eficacia.

3. Para los abogados que participan en la defensa o persecución de casos de fraude informático en el distrito fiscal del Callao, se recomienda desarrollar un conocimiento exhaustivo sobre las tipologías de delitos informáticos y su relación con las modalidades de fraude digital. Con una comprensión detallada de cómo los delitos informáticos evolucionan en respuesta a las medidas de control, los abogados podrán diseñar estrategias legales más sólidas y fundamentadas que permitan tanto anticiparse a nuevas prácticas delictivas como consolidar sus argumentaciones frente a los tribunales. Este enfoque estratégico fortalecerá la calidad de los procesos judiciales y facilitará la adecuada protección de los derechos de las partes involucradas.

4. Para los abogados involucrados en casos de fraude informático en el distrito fiscal del Callao, es recomendable ampliar sus conocimientos en Tecnologías de la Información y Comunicación (TIC), dada su relevancia en el desarrollo y ejecución de estrategias de defensa y acusación en este tipo de delitos. El entendimiento profundo de las TIC permitirá a los abogados identificar con mayor precisión los mecanismos técnicos que facilitan el fraude informático, contribuyendo a construir argumentos legales basados en pruebas de carácter tecnológico. Esta capacitación técnica será un recurso clave para sustentar pruebas periciales y defender con mayor contundencia los intereses de sus clientes, adaptándose a los desafíos específicos de los delitos cibernéticos actuales.

VII. Referencias bibliográficas

Alcántara, F. (2024). *Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022* [Informe de pregrado]. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/12384/Alcantara%20Diaz%2c%20Fabian%20Eduardo.pdf?sequence=1&isAllowed=y

Arellano, G. y Galindo, S. (2022). *Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático, Lima 2019 – 2021* [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/102672/Arellano_CGL-Galindo_MSE-SD.pdf?sequence=4&isAllowed=y

Astaiza, P. y Cuellar, V. (2023). *Análisis dogmático de los delitos informáticos o ciberdelitos en Colombia* [Informe de pregrado]. Universidad Libre Seccional Cali. https://repository.unilibre.edu.co/bitstream/handle/10901/29295/An%c3%a1lisis%20Dogm%c3%a1tico%20de%20los%20Delitos%20Inform%c3%a1ticos%20o%20Ciberdelitos%20en%20Colombia.pdf?sequence=3&isAllowed=y

Calva, Y. y Nivelo, E. (2021). *Tratamiento de los delitos informáticos en el código orgánico integral penal* [Informe de pregrado]. Universidad Regional Autónoma De Los Andes. https://dspace.uniandes.edu.ec/bitstream/123456789/14110/1/USD-DER-EAC-090-2021.pdf

Carrera, I. (2021). *Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021* [Informe de posgrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/71492/Carrera_PIDR-SD.pdf?sequence=1&isAllowed=y

Chumbe, B. (2023). *Fraude informático frente a la libertad de empresa como garantía constitucional, Lima, 2023* [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/131274/Chumbe_HBB-SD.pdf?sequence=1&isAllowed=y

Custodio, Y. (2021). *Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático* [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74797/Custodio_CY-SD.pdf?sequence=1&isAllowed=y

De la Cruz, W. y Lulli, J. (2023). *Tratamiento de los casos de delitos informáticos contra el patrimonio en el Distrito Fiscal del Santa, 2022* [Informe de pregrado]. Universidad César Vallejo.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/131745/DelaCruz_CWA-Lulli_CJA-SD.pdf?sequence=1&isAllowed=y

Delgado, F. (2022). *El tratamiento penal de los delitos informáticos contra el patrimonio de las personas naturales y jurídicas en la Corte Superior de Justicia del Santa – Chimbote* [Informe de pregrado]. Universidad Señor de Sipán. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10400/Delgado%20Benites%2c%20Francisco%20Javier.pdf?sequence=1&isAllowed=y

Dia, I., Ojeda, P., Cajas, C. y Cabrera, E. (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

Espinoza, J. (2022). *Factores que inciden en la tipicidad objetiva del delito de fraude informático, Ministerio Público Chepén, 2022* [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/114016/Espinoza_MJC-SD.pdf?sequence=1&isAllowed=y

Guillén, O.; Sánchez, M. y Begazo, L. (2020). *Pasos para elaborar una tesis de tipo correlacional, bajo el enfoque cuantitativo, variable categórico, escala ordinal y la estadística no paramétrica.* Editorial CLIIC. https://cliic.org/2020/Taller-Normas-APA-2020/libro-elaborar-tesis-tipo-correlacional-octubre-19_c.pdf

Lujan, Z. (2022). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio y la fe pública en el Distrito Judicial de Lima, 2022* [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/89722/Lujan_CZT-SD.pdf?sequence=1&isAllowed=y

Malca, E. (2023). *Eficacia de la persecución penal en la investigación preparatoria del delito de fraude informático, Callao, 2022* [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/129112/Malca_LEC-SD.pdf?sequence=1&isAllowed=y

Ramos, M. y Salvador, Y. (2022). La regulación de las nuevas modalidades del delito informático en la ley N° 30096 y su modificatoria, periodo 2020-2021 [Informe de pregrado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/108873

Tauche, S. (2022). *Actos de investigación y tratamiento normativo en los delitos de fraude informático, Distrito Fiscal de Lima Sur, 2021* [Informe de pregrado]. Universidad San Pedro.

https://repositorio.usanpedro.edu.pe/server/api/core/bitstreams/28d85917-8d90-4732-810e-5b2b552f53cb/content

VIII. Anexos

Anexo 1 Instrumento de recolección de datos

Tratamiento político - normativo del fraude informático, Distrito Fiscal Del Callao, 2020-2022

Instrucciones: La finalidad de esta encuesta es Determinar la relación entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022

Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

TRATAMIENTO POLÍTICO - NORMATIVO

N°	Pregunta	1	2	3	4	5
	Ley N° 30096					
1.	¿Considera que la Ley N° 30096 ha sido adecuadamente implementada para abordar los desafíos del fraude informático en el contexto peruano?					
2.	¿Cree que las actuales regulaciones y políticas bajo la Ley N° 30096 se están cumpliendo de manera efectiva para prevenir el fraude informático?					
3.	¿Opina que las autoridades competentes han proporcionado suficientes recursos y formación para garantizar la correcta implementación de la Ley N° 30096 en la lucha contra el fraude informático?					
4.	¿Estima que las sanciones contempladas en la Ley N° 30096 son adecuadas y se están aplicando de manera justa para disuadir las prácticas de fraude informático?					
5.	¿Juzga que la Ley N° 30096 incluye suficientes mecanismos de actualización para adaptarse a las nuevas modalidades de fraude informático que surgen con los avances tecnológicos?					
	Delito informático					
6.	¿Considera que la actual legislación en torno al delito informático es suficiente para reducir de manera significativa la incidencia de fraudes cibernéticos en el país?					
7.	¿Cree que las medidas normativas implementadas son adecuadas para proteger las infraestructuras críticas y minimizar la explotación de vulnerabilidades en el ámbito informático?					

8.	¿Opina que las políticas actuales de combate contra el delito informático han logrado una disminución efectiva en la frecuencia de estos delitos?	
9.	¿Juzga que las estrategias adoptadas por el gobierno para fortalecer la ciberseguridad son efectivas para prevenir la explotación de vulnerabilidades en los sistemas informáticos?	
10.	¿Estima que el marco legal vigente es suficientemente robusto para hacer frente a la evolución constante de las técnicas utilizadas en el fraude informático?	
	Tecnología de la información y comunicación	
11.	¿Considera que las políticas normativas actuales fomentan adecuadamente la adopción de tecnologías de la información y comunicación para prevenir el fraude informático?	
12.	¿Cree que los marcos regulatorios vigentes son efectivos para garantizar una seguridad informática robusta frente a las amenazas del fraude digital?	
13.	¿Opina que la legislación en materia de tecnología de la información y comunicación está alineada con las necesidades tecnológicas modernas para combatir el fraude cibernético?	
14.	¿Juzga que las medidas de seguridad informática establecidas en las normativas actuales son suficientes para proteger los datos sensibles contra el fraude?	
15.	¿Estima que las iniciativas gubernamentales han sido efectivas en promover la integración de tecnologías avanzadas en la lucha contra el fraude informático?	

FRAUDE INFORMÁTICO

N°	Pregunta	1	2	3	4	5
	Tratamiento normativo					
1.	¿Considera que el marco regulatorio actual es suficiente para abordar eficazmente las diversas formas de fraude informático que afectan al país?					
2.	¿Cree que la aplicación de las normativas vigentes ha sido adecuada para prevenir y sancionar de manera efectiva los delitos informáticos?					
3.	¿Opina que las leyes existentes necesitan actualizaciones para mantenerse al día con los rápidos avances tecnológicos que facilitan el fraude informático?					
4.	¿Juzga que las autoridades encargadas de la implementación y aplicación de las leyes contra el fraude informático están cumpliendo con sus responsabilidades de manera efectiva?					
5.	¿Estima que el tratamiento normativo dado al fraude informático es suficientemente exhaustivo para cubrir todas las posibles brechas de seguridad cibernética?					
	Modalidades					
6.	¿Considera que las normativas actuales contemplan adecuadamente la diversidad de tipos de fraude informático que existen en el entorno digital?					
7.	¿Cree que las estrategias normativas vigentes son efectivas para contrarrestar los métodos de ataque informático más sofisticados y en constante evolución?					
8.	¿Opina que las legislaciones actuales abordan de manera integral las diferentes modalidades de fraude cibernético que afectan a los usuarios y a las empresas?					

9.	¿Juzga que las autoridades han implementado medidas adecuadas para prevenir y responder a los métodos de ataque informático emergentes?	
10.	¿Estima que las políticas públicas en vigor están suficientemente preparadas para hacer frente a las nuevas variantes de fraude informático que surgen con el avance de la tecnología?	

Gracias por su colaboración

Anexo 2 Matriz de consistencia

Problemas de investigación	Objetivos de investigación	Hipótesis de investigación	Variables	Metodología
Problema general	**Objetivo general**	**Hipótesis general**	**Variable 1**	**Tipo de investigación** Tipo básica **Enfoque de investigación** Cuantitativo **Nivel de investigación:** Relacional **Diseño de la investigación:** No experimental **Población y muestra** **Población:** 81 operadores de justicia **Muestra:** 81 operadores de justicia **Tipo de muestra** No probabilística Muestreo por conveniencia **Técnica de recolección de datos** Encuesta **Instrumento** Cuestionario
¿Cuál es la relación entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022?	Determinar la relación entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022	Existe relación significativa entre el tratamiento político – normativo y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022	Tratamiento político - normativo	
Problemas específicos	**Objetivos específicos**	**Hipótesis específicas**	**Dimensiones**	
• ¿Cuál es la relación entre la dimensión Ley N° 30096 y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022? • ¿Cuál es la relación entre la dimensión delito informático y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022? • ¿Cuál es la relación entre la dimensión tecnología de la información y comunicación y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022?	• Establecer la relación entre la dimensión Ley N° 30096 y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022 • Establecer la relación entre la dimensión delito informático y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022 • Establecer la relación entre la dimensión tecnología de la información y comunicación y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022	• Existe relación significativa entre la dimensión Ley N° 30096 y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022 • Existe relación significativa entre la dimensión delito informático y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022 • Existe relación significativa entre la dimensión tecnología de la información y comunicación y el fraude informático, Distrito Fiscal del Callao, 2020 – 2022	Ley N° 30096 Delito informático Tecnología de la información y comunicación **Variable 2** Fraude informático **Dimensiones** Tratamiento normativo Modalidades	

Anexo 3 Cuadro de operacionalización de variables

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala	Instrumento
Variable 1 Tratamiento político - normativo	Se refiere a la forma en la que las políticas y normativas gubernamentales llegan a ser desarrolladas con la finalidad de regular determinados criterios dentro de una sociedad (Arellano y Galindo, 2022).	Por medio del cuestionario, especialistas en derecho ofrecieron sus valoraciones acerca de la realidad del tratamiento que se le da al fraude informático.	Ley N° 30096	Implementación normativa Cumplimiento regulatorio	Ordinal	Cuestionario
			Delito informático	Incidencia delictiva Vulnerabilidad explotada		
			Tecnología de la información y comunicación	Adopción de tecnologías Seguridad informática		
Variable 2 Fraude informático	Queda concebido como aquella manipulación o alteración que se llega a realizar de los sistemas informáticos, con el objetivo de alcanzar beneficios económicos o causar daño a determinadas personas (Tauche, 2022).	Se valoró por medio del empleo del cuestionario aplicado hacia especialistas en derecho, con la finalidad de entender la normatividad y las formas de delito que puede llegar a controlar de acuerdo con la realidad nacional.	Tratamiento normativo	Marco regulatorio Aplicación legal	Ordinal	Cuestionario
			Modalidades	Tipos de fraude Métodos de ataque		

Anexo 4 Ficha técnica de instrumento

Variable: Tratamiento político - normativo

Universidad: Universidad César Vallejo

Autor: Arellano Casimiro, Gisela Lisset / Galindo Martinez, Sofia Emilia

Año: 2022

Lugar: Perú

Título: Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático, Lima 2019 – 2021

Duración: 20 minutos

Valoración: Para la presente investigación, se ha considerado la escala Likert de valoración

Confiabilidad del instrumento: La confiabilidad del presente instrumento, se ha encontrado determinado, por medio del Alfa de Cronbach, en el que se alcanzó una valoración mayor a 0.70

Profesionales validadores: Mg. Vásquez Torres, Arturo Rafael

Link: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/102672/Arellano_CGL-Galindo_MSE-SD.pdf?sequence=4&isAllowed=y

Variable: Fraude informático

Universidad: Universidad San Pedro

Autor: Tacuche Rodriguez, Shirley Carolina

Año: 2022

Lugar: Perú

Título: Actos de investigación y tratamiento normativo en los delitos de fraude informático, Distrito Fiscal de Lima Sur, 2021

Duración: 20 minutos

Valoración: Para la presente investigación, se ha considerado la escala Likert de valoración

Confiabilidad del instrumento: La confiabilidad del presente instrumento, se ha encontrado determinado, por medio del Alfa de Cronbach, en el que se contó con una valoración mayor a 0.70

Profesionales validadores: Urcia Quispe, Manuel Ulises

Link: https://repositorio.usanpedro.edu.pe/server/api/core/bitstreams/28d85917-8d90-4732-810e-5b2b552f53cb/content

Anexo 5 Base de datos

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
5	4	4	3	4	5	3	4	3	3	4	3	4	5	3	5	5	4	5	5	5	4	5	5	5
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	3	3	3	3	4	4	4	4	4	3	3	3	4	4	4	5	4	4	5	4	5	5	5	5
1	1	1	1	3	3	3	2	2	4	3	2	3	3	3	3	2	2	3	3	2	2	3	3	2
2	4	3	3	2	1	3	1	3	2	1	1	1	1	4	3	3	2	4	4	4	3	3	2	3
3	3	3	3	3	3	2	1	4	4	3	3	3	3	2	3	2	3	4	3	2	3	3	4	2
2	3	2	3	3	3	4	2	3	3	2	3	3	3	4	2	3	4	3	2	4	3	3	3	3
2	1	2	2	1	1	2	2	2	3	1	1	3	2	3	2	3	3	3	1	2	2	1	2	1
3	3	2	3	3	2	2	1	3	3	2	3	1	1	3	3	2	2	2	2	2	2	2	3	3
2	1	1	2	1	2	3	3	3	3	2	1	3	1	2	1	1	1	2	3	3	2	2	3	2
3	3	1	3	3	3	1	2	3	1	2	3	2	2	1	3	1	3	2	3	2	1	1	3	1
2	3	3	1	3	1	3	1	3	2	2	3	2	1	1	3	2	1	1	3	2	3	1	2	1
3	2	3	2	3	3	3	1	3	1	2	3	1	1	1	2	2	1	1	1	2	2	2	2	2
1	2	2	3	2	2	2	2	3	3	1	3	1	3	3	2	2	2	3	2	1	3	3	1	3
1	3	2	2	3	3	2	1	3	2	1	3	1	3	3	1	1	3	1	2	2	1	3	1	2
3	2	4	4	2	4	2	4	4	4	4	4	2	4	2	3	2	3	3	1	4	4	3	3	2
1	3	3	3	2	3	3	2	3	3	3	3	2	3	3	3	2	3	3	3	2	4	4	3	4
3	4	2	2	3	3	3	1	4	4	2	2	3	3	3	4	3	4	2	2	3	2	3	2	2
3	2	4	5	3	3	2	4	4	4	4	5	3	3	2	2	2	1	4	3	3	3	1	4	3
4	3	3	2	4	2	1	4	3	3	3	2	4	2	4	2	1	3	3	3	3	4	2	4	3
3	3	2	4	4	4	3	2	3	4	2	4	4	4	3	2	2	1	4	3	3	3	2	4	4
5	4	4	3	4	5	3	4	3	3	4	3	4	5	3	5	5	4	5	5	5	4	5	5	5
1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	1	1	1	1	1	1	1	1	1	1
2	3	3	3	3	4	4	4	4	4	3	3	3	4	4	4	5	4	4	5	4	5	5	5	5
3	3	3	2	3	1	3	1	1	1	1	1	2	1	3	1	1	1	2	3	3	2	3	1	3
3	3	2	3	2	1	1	2	2	1	2	2	3	3	1	1	1	1	1	2	1	1	1	3	3
1	1	2	2	3	2	1	2	1	2	2	1	3	1	3	1	2	1	3	3	1	2	1	3	3
3	2	3	3	1	1	3	1	2	1	3	1	1	1	3	3	3	3	1	1	1	1	1	1	2
3	2	2	2	2	1	2	2	3	2	2	1	2	2	2	3	1	1	3	2	2	1	1	1	3
1	1	3	2	1	1	1	3	1	1	1	2	1	2	2	3	3	2	2	1	3	1	1	1	2
3	1	3	3	1	3	1	3	1	1	2	2	2	2	3	3	2	1	2	3	1	2	2	2	3
3	1	2	1	3	2	2	2	2	3	2	1	2	3	1	1	3	3	3	2	2	3	1	3	2
3	1	2	2	2	2	1	2	3	1	3	2	1	1	1	3	1	1	3	3	1	2	3	3	1
1	3	3	2	1	1	2	1	3	1	1	1	2	3	3	2	1	3	1	2	2	2	1	3	1
2	1	2	1	2	1	3	1	2	1	2	2	2	1	2	3	3	2	3	2	2	3	1	3	2
2	3	1	2	2	2	3	1	2	1	2	2	2	3	2	2	3	2	1	1	3	3	1	3	2
3	1	3	1	1	2	3	2	1	2	3	2	2	2	1	2	1	1	1	2	1	2	1	3	2
2	3	2	3	2	3	3	3	2	2	3	3	2	3	2	3	3	3	2	2	3	2	3	3	1
1	2	2	3	2	1	2	1	3	2	2	1	1	1	2	2	1	1	1	2	3	2	1	1	1
3	2	2	2	3	3	3	3	2	1	2	1	2	1	3	2	2	1	3	1	1	3	1	2	2
3	3	2	3	1	1	2	2	3	1	2	2	3	3	2	3	1	3	2	1	3	1	3	2	1
1	2	2	2	2	3	1	1	1	2	2	1	1	2	2	2	1	1	1	1	2	2	1	2	1
2	3	2	3	2	3	2	2	4	3	3	4	3	3	3	3	3	3	2	3	3	2	4	4	4
2	2	3	4	3	2	3	2	4	3	3	3	4	3	2	3	3	2	3	4	3	3	3	3	4
3	4	3	3	2	4	2	4	2	3	2	3	3	4	4	2	3	2	4	4	4	3	2	4	3
4	3	3	2	4	3	4	3	3	3	2	2	2	4	4	2	3	3	2	3	4	3	4	4	4
3	4	4	2	3	2	2	2	2	4	2	4	3	4	2	3	3	4	4	4	4	4	3	4	3
2	4	3	4	4	3	2	4	4	3	3	3	3	3	2	4	4	3	2	4	2	2	4	3	4
2	3	3	3	3	2	4	2	3	3	2	2	4	3	4	4	2	4	4	2	2	2	2	3	3
3	2	2	4	2	2	4	3	3	2	4	4	3	3	4	4	4	3	4	4	2	4	2	3	3
2	4	2	3	4	3	3	4	2	4	4	4	4	3	4	3	2	4	3	2	3	4	4	3	4
2	4	4	4	2	2	2	4	4	2	3	4	2	3	4	3	4	2	2	2	4	4	4	4	2
1	3	2	2	1	3	2	2	2	1	1	1	3	3	2	2	3	2	3	1	1	3	2	3	2
2	3	1	3	2	2	2	2	1	2	1	1	3	2	3	1	3	2	3	3	3	2	1	1	3
1	1	1	2	2	2	2	1	2	1	2	2	2	3	3	2	1	3	1	1	1	2	3	3	1
2	2	3	4	2	4	4	3	3	2	4	2	4	4	2	3	4	2	4	3	3	3	2	3	3
3	4	2	3	2	3	3	4	2	3	4	4	2	3	4	4	3	4	3	4	4	2	3	3	4
4	4	4	3	4	3	2	2	3	2	2	3	3	2	2	3	2	3	4	2	3	3	3	3	3
2	4	2	3	3	3	2	2	4	3	4	3	2	4	4	4	3	4	3	2	3	3	3	4	4
3	2	3	3	4	2	4	2	2	2	3	4	2	4	2	2	3	4	4	3	3	2	2	4	4

Anexo 6 Confiabilidad del instrumento

VARIABLE 1

N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	
1	2	1	1	1	2	2	1	2	2	2	2	1	1	2	2	24.00
2	2	2	2	1	2	2	1	1	2	1	2	1	2	2	1	24.00
3	1	1	1	2	2	1	1	2	2	1	1	2	2	2	1	22.00
4	4	4	4	2	4	2	3	4	3	3	4	3	3	4	4	51.00
5	2	4	3	3	2	2	4	3	3	2	2	4	3	3	2	42.00
6	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	45.00
7	3	1	1	2	2	1	3	3	1	3	1	2	1	1	2	27.00
8	3	3	3	3	3	3	3	2	3	1	3	3	3	2	2	40.00
9	2	2	3	2	4	2	2	3	2	4	2	2	3	2	4	39.00
10	3	2	3	3	3	3	2	3	3	3	3	2	3	3	3	42.00
Varianzas	0.65	1.21	1.04	0.56	0.61	0.49	1.01	0.64	0.44	1.01	0.81	0.81	0.64	0.64	1.04	96.64

K (Número de ítems)	15.000
Vi varianza por item	11.600
Vt (varianza total)	96.640
Alfa	0.943

VARIABLE 2

N°	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	
1	1	1	2	2	2	1	1	2	2	2	16.00
2	1	1	2	1	2	1	2	1	1	2	14.00
3	1	2	1	1	1	2	2	1	2	2	15.00
4	2	3	2	3	4	3	2	3	3	2	27.00
5	3	3	2	4	4	2	4	3	3	2	30.00
6	3	2	3	4	3	3	3	3	3	3	30.00
7	3	1	2	2	2	1	3	3	2	2	21.00
8	2	1	1	1	1	2	2	3	1	1	15.00
9	2	3	2	4	4	2	2	3	2	4	28.00
10	3	2	3	3	2	3	2	3	3	3	27.00
Varianzas	0.69	0.69	0.40	1.45	1.25	0.60	0.61	0.65	0.56	0.61	41.21

K (Número de ítems)	10.000
Vi varianza por item	7.510
Vt (varianza total)	41.210
Alfa	0.909

AMBAS VARIABLES

N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	
1	2	1	1	1	2	2	1	2	2	2	2	1	1	2	2	1	1	2	2	2	1	1	2	2	2	40.00
2	2	2	2	1	2	2	1	1	2	1	2	1	2	2	1	1	1	2	1	2	1	2	1	1	2	38.00
3	1	1	1	2	2	1	1	2	2	1	1	2	2	2	1	1	2	1	1	1	2	2	1	2	2	37.00
4	4	4	4	2	4	2	3	4	3	3	4	3	3	4	4	2	3	2	3	4	3	2	3	3	2	78.00
5	2	4	3	3	2	2	4	3	3	2	2	4	3	3	2	3	3	2	4	4	2	4	3	3	2	72.00
6	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	4	3	3	3	3	3	3	75.00
7	3	1	1	2	2	1	3	3	1	3	1	2	1	1	2	3	1	2	2	2	1	3	3	2	2	48.00
8	3	3	3	3	3	3	3	2	3	1	3	3	3	2	2	2	1	1	1	1	2	2	3	1	1	55.00
9	2	2	3	2	4	2	2	3	2	4	2	2	3	2	4	2	3	2	4	4	2	2	3	2	4	67.00
10	3	2	3	3	3	3	2	3	3	3	3	2	3	3	3	3	2	3	3	2	3	2	3	3	3	69.00
Varianzas	0.65	1.21	1.04	0.56	0.61	0.49	1.01	0.64	0.44	1.01	0.81	0.81	0.64	0.64	1.04	0.69	0.69	0.40	1.45	1.25	0.60	0.61	0.65	0.56	0.61	236.09

K (Número de ítems)	25.000
Vi varianza por item	19.110
Vt (varianza total)	236.090
Alfa	0.957

Anexo 7 Baremos

Tabla 7

Baremos de variables y dimensiones

	Nivel bajo	Nivel medio	Nivel alto
Variable 1	15 - 35	36 – 55	56 – 75
Variable 2	10 – 23	24 – 36	37 - 50
Dimensiones	5 – 11	12 – 17	18 - 25