Universidad Continental

FACULTAD DE DERECHO

Escuela Académico Profesional de Derecho

Tesis

Delito de suplantación de identidad y los medios informáticos, Lima, periodo 2023-2024

Mayra Yessenia Sanchez Espejo

Para optar el Título Profesional de Abogada

Lima, 2025

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A	**:**	Decana de la Facultad de Derecho
DE	**:**	Betty Antonia Flores Vila Asesora de trabajo de investigación
ASUNTO	**:**	Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA	**:**	07 de diciembre de 2025

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesora del trabajo de investigación:

Título:
DELITO DE SUPLANTACIÓN DE IDENTIDAD Y LOS MEDIOS INFORMÁTICOS, LIMA, PERIODO 2023-2024

Autora:
Mayra Yessenia Sanchez Espejo – Carrera profesional Derecho

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 17 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía SI [x] NO [ ]
- Filtro de exclusión de grupos de palabras menores SI [x] NO [ ]
  Nº de palabras excluidas **(en caso de elegir "SI")**: 25
- Exclusión de fuente por trabajo anterior del mismo estudiante SI [ ] NO [x]

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre la autora y asesora, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

La firma del asesor obra en el archivo original
(No se muestra en este documento por estar expuesto a publicación)

DEDICATORIA

Para mis padres, quienes fueron los que me brindaron apoyo en mi educación sin mediar reparos. Cuanto obtenga en mi largo caminar de la vida siempre será gracias a ellos.

AGRADECIMIENTO

A Dios, por brindar fuerzas y buena salud a mis padres para que puedan llevar adelante el forjamiento de mi educación. Y mi familia, que me da el soporte para seguir mis objetivos.

RESUMEN

La presente investigación analiza los delitos de suplantación de identidad y los medios informáticos con el propósito de determinar cómo el uso de estos influye en el delito de suplantación de identidad, en Lima, en el periodo 2023-2024. La metodología empleada fue cuantitativa, básica, de alcance descriptivo y diseño no experimental-transeccional. Además se utilizó como herramienta de recolección de datos dos cuestionarios con una muestra de 15 efectivos de la DIRINCRI especialistas en el área de delitos informáticos y 10 modalidades de delitos contra el patrimonio. Por lo tanto, se contó con 28 ítems, que luego fueron analizados por el software estadístico SPSS. Los resultados evidenciaron una correlación positiva alta con un coeficiente de Pearson r=0.808 y un nivel de significancia de p=0.00, inferior al umbral establecido en 0.05. Se concluyó que los medios informáticos influyen de manera significativa en el delito de suplantación de identidad en Lima, durante el periodo 2023-2024, por lo que muestran la necesidad de fortalecer las medidas de ciberseguridad y la protección de datos personales en entornos.

Palabras clave: Medios informáticos, delito de suplantación de identidad, datos personales.

ABSTRACT

This research analyzes identity theft crimes and computer media, with the purpose of determining how the use of computer media influences the crime of identity theft, Lima, period 2023-2024. The methodology used was quantitative, basic, descriptive in scope, and non-experimental-transectional in design. Two questionnaires were also used as data collection tools with a sample of 15 DIRINCRI personnel specialized in cybercrimes and 10 types of property crimes. Therefore, 28 items were collected, which were then analyzed using SPSS statistical software. The results showed a high positive correlation with a Pearson coefficient of r = 0.808 and a significance level of p = 0.00, lower than the threshold set at 0.05. It was concluded that cybersecurity significantly influenced the crime of identity theft in Lima during the 2023-2024 period, highlighting the need to strengthen cybersecurity measures and the protection of personal data in these environments.

Key words: Computer media, identity theft crime, personal data.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

El entorno que nos rodea se encuentra en constantes cambios e innovaciones tecnológicas, los cuales ha traído una serie de ventajas para las personas. Sin embargo, este cambio acelerado ha generado algunos problemas que han afectado la seguridad y resquebrajado algunas leyes. Esto se debe a la gran cantidad de información que circula día tras día, haciendo que las personas la usen en su conveniencia y buscando siempre un beneficio personal.

En la actualidad, acceder a cualquier tipo de información es una acción relativamente sencilla, a diferencia de años atrás, cuando no existía una armonía digital y tecnológica. Como consecuencia de esta gran revolución, han surgido nuevos delitos que no estaban contemplados en la normativa vigente. Frente a ello, las autoridades y las cartas magnas han tenido que actualizarse y supervisar de cerca estos nuevos problemas. Uno de los delitos que más preocupación viene generando es la usurpación de identidad, el cual, pese a contar con una sanción en el derecho penal, no ha dejado de incrementarse en distintos países.

Por eso este trabajo tiene como objetivo investigación determinar cómo el uso de los medios informáticos influye en el delito de suplantación de identidad, en Lima, en el periodo 2023-2024. Para investigar este fin fue necesario dividir el trabajo en 6 capítulos:

El capítulo I aborda un breve panorama del tema de investigación. El capítulo II desarrolla el planteamiento de problemas y objetivos del estudio, así como la justificación, importancia, alcances y limitaciones. El capítulo III evidencia los antecedentes internacionales y naciones relacionados a las variables de estudio, teorías, definiciones y contrastes del tema investigado. El capítulo IV muestra las hipótesis de investigación y las variables. El capítulo V

aborda la metodología de estudio, el tipo, enfoque, alcance, diseño, población y muestra, y las técnicas de recolección de datos. Y el capítulo VI evidencia los resultados del estudio tras la recolección de información y el contraste de las hipótesis.

Finalmente se detallan algunas conclusiones y recomendaciones para hacer frente al problema de investigación, acompañado de las referencias utilizadas en el estudio y los anexos respectivos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Planteamiento y delimitación del problema

La OEA (2022), desde un contexto global, ha evidenciado una preocupante falta de capacidad en ciberseguridad, particularmente en regiones como África, América Latina y el Caribe. En 2017, África reportó una pérdida aproximada de 3,700 millones de dólares a causa de la ciberdelincuencia, en tanto más del 90 % de sus empresas operaban por debajo del umbral mínimo de seguridad cibernética. Esto refleja una clara falta de preparación que deja a las comunidades más vulnerables expuestas a mayores riesgos, limita su capacidad para aprovechar plenamente las tecnologías de la información y las comunicaciones, y genera una ausencia de resiliencia y garantías en la protección de su seguridad y privacidad digital, poniendo en peligro la sostenibilidad de los proyectos de desarrollo y evidenciando la necesidad urgente de que la ciberseguridad sea contemplada desde el inicio en la planificación y ejecución de políticas de desarrollo.

INAI (2023) señala que en México los avances en Inteligencia Artificial, junto con el uso indebido de datos personales, han facilitado que ciberdelincuentes suplan la identidad de las personas. Esto se ha convertido en una amenaza creciente, al registrarse un incremento del 218 % en los casos de usurpación de identidad mediante esta tecnología en el último año, con un total de mil 607 reportes entre enero y octubre de 2023. De esto, el 62 % corresponde al hackeo de información en redes sociales, el 26 % al robo de datos desde teléfonos móviles y el 2 % a la clonación de tarjetas bancarias o falsificación de firmas. Eso evidencia una urgente necesidad de adoptar medidas preventivas que reduzcan la exposición de información personal y refuercen la protección de la identidad digital.

En el Perú, el Ministerio de Justicia y Derechos Humanos (2022) ha evidenciado un preocupante aumento en los casos de suplantación de identidad, los cuales pasaron de 935 denuncias en 2020 a 2,666 en 2021, y representa el 18.2 % del total de ciberdelitos registrados ese año y se posiciona como la segunda modalidad más frecuente en 2020 y la primera en 2021, por encima de otras formas de ciberdelincuencia. Asimismo, durante enero y febrero de 2025 se registró 1,406 casos de suplantación de identidad, lo que equivale al 22 % del total de ciberdelitos en ese periodo, y se consolida nuevamente como la segunda modalidad más reportada a nivel nacional (Verano, 2025). Por otro lado, según RENIEC (2024), entre 2020 y la fecha se han bloqueado 923 intentos de suplantación de identidad en procesos de inscripción del DNI, muchos de ellos utilizando datos de personas fallecidas. Asimismo, se ha identificado más de 333,000 trámites irregulares y se ha bloqueado más de 3.8 millones de intentos de ciberataques, incluidos 2.3 millones de validaciones automatizadas mediante redes de bots. Esto refleja la creciente amenaza de la ciberdelincuencia y el tráfico ilegal de datos personales, y resalta la necesidad urgente de una respuesta estatal coordinada y tecnológica para proteger la identidad digital de los ciudadanos peruanos.

Finalmente, desde un enfoque local, la Dirección de Investigación Criminal de la Policía Nacional del Perú (DIRINCRI PNP) ha reportado un número considerable de denuncias por delitos informáticos desde el año 2020, siendo la cifra más reciente la del 2024, con un total de 3,058 casos. De estos, 726 corresponden a suplantación de identidad, lo que la posiciona como la segunda modalidad delictiva más frecuente en la capital.

De esa manera se percibe que la presencia de los medios informáticos en la vida diaria de las personas en Lima ha traído consigo un impacto preocupante en el que cada vez más ciudadanos se ven afectados por el delito de suplantación de identidad. Esta situación ha ido en aumento debido al uso masivo de redes sociales, plataformas digitales y servicios en línea,

los cuales aunque ofrecen múltiples beneficios también han abierto la puerta a que ciberdelincuentes accedan con facilidad a datos personales, los manipulen y los utilicen con fines maliciosos como hacerse pasar por alguien más, lo que vulnera la privacidad de las personas y puede alterar gravemente su vida personal, profesional y financiera, tal como se refleja en el alarmante número de denuncias registradas en la capital.

1.2. Formulación del problema

1.2.1 Pregunta general

- ¿Cómo el uso de los medios informáticos influye en el delito de suplantación de identidad, Lima, periodo 2023-2024?

1.2.2 Preguntas específicas

- ¿Cómo el uso de los medios informáticos influye en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024?
- ¿Cómo el uso de los medios informáticos influye en la transferencia o cesión de datos personales, Lima, periodo 2023-2024?
- ¿Cómo el uso de los medios informáticos influye en la utilización de datos personales, Lima, periodo 2023-2024?

1.3. Objetivos de la Investigación

1.3.1 Objetivo principal

- Determinar cómo el uso de los medios informáticos influye en el delito de suplantación de identidad, Lima, periodo 2023-2024.

1.3.2 Objetivos específicos

- Determinar cómo el uso de los medios informáticos influye en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.

- Determinar cómo el uso de los medios informáticos influye en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.
- Determinar cómo el uso de los medios informáticos influye en la utilización de datos personales, Lima, periodo 2023-2024.

1.4. Justificación e importancia del estudio

El estudio en todo momento recolectó información real y actual de las variables de estudio. Por ello evidencia la integración de la teoría del delito, la estructura del mismo y cómo se viene cometiendo en la sociedad. En el aspecto metodológico, se optó por un estudio cuantitativo, ya que solo así las variables podrían ser analizadas de forma exacta en el contexto planteado. En cuanto a la justificación legal, este delito se encuentra estipulado en la Ley N°30096. Sin embargo, luego fue modificada con la Ley N°30171, donde se analiza la naturaleza jurídica de forma exacta, de modo que permite comprender cómo deben actuar las autoridades respecto a este problema y cómo la sociedad civil puede actuar frente a esto.

1.4.1 Alcances

Esta investigación busca ahondar más en el delito de falsificación de identidad con la influencia de los medios informáticos, de manera que con lo hallado se pueda conocer más al respecto. Asimismo, con base en los resultados estadísticos, se busca evidenciar la magnitud de este delito en la sociedad peruana, de modo que se planteen nuevas soluciones y medidas para proteger y educar a las personas. Otro punto importante es que la presente investigación posee fuentes oficiales de la DIRINCRI y, con ella, se desea mostrar que los delitos informáticos vienen afectando a gran parte de la población en sus diversas formas de operación. Por ello es necesario establecer algunas recomendaciones para hacer frente a este y así evitar que existan más víctimas o personas que ignoran cómo protegerse y cómo reconocer hechos que podrían perjudicarlos a corto o largo plazo.

1.4.2 Limitaciones

La investigación presentó algunas limitaciones en la recolección de cifras exactas, ya que se requería información muy detallada exclusivamente de Lima, lo que dificultó el acceso a datos precisos y actualizados. Además, debido a la naturaleza especializada de los delitos cibernéticos, fue necesario obtener información directamente de especialistas en ciberseguridad dentro de la DIRINCRI, quienes manejan reportes internos y clasificados. La disponibilidad de estos datos dependía de procesos de validación y autorización, lo que hizo que el acceso a fuentes oficiales fuera más complejo y prolongado.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1 Antecedentes internacionales

El delito de suplantación de identidad es un problema que actualmente no afecta únicamente al Perú. Esto se evidencia en estudios previos realizados en países de la región, donde se ha determinado un gran índice de porcentaje en phishing.

Según Harán (2021), el 40 % de las empresas en América Latina reportó infecciones de malware, afectando principalmente a Brasil (19 %), México (17.5 %), Argentina (13.3 %), Colombia (10.6 %) y Perú (8.9 %). Además, un estudio de Kaspersky (2023) reveló que, entre junio de 2022 y julio de 2023, se registró 1,190 millones de intentos de infección de malware en la región, con Brasil liderando con 1,515 bloqueos por minuto, seguido de México (275), Colombia (117) y Perú (107). Estas cifras reflejan el creciente impacto del malware en Sudamérica.

a) Ecuador. Macías et al. (2024) llevaron a cabo una investigación con un enfoque cualitativo para destacar la importancia de combatir la suplantación de identidad en la sociedad actual. Los resultados evidenciaron que este delito puede presentarse de diversas formas en las redes sociales, generando riesgos significativos para la información personal y la reputación de los usuarios. La investigación subraya que proteger los datos del usuario y la prevención de fraudes no solo deben ser una prioridad individual, sino también una responsabilidad clave para instituciones financieras, empresas y gobiernos. Esto implica fortalecer las medidas de seguridad digital y fomentar una mayor conciencia pública sobre este problema para reducir su impacto.

Díaz et al. (2022) realizaron un análisis jurídico sobre la responsabilidad bancaria ante los delitos informáticos, empleando una metodología cuantitativa de tipo documental-bibliográfica. Mediante la revisión documental y la observación de la situación social, los investigadores llegaron a reflexiones importantes. Señalan que, aunque el uso de Internet permite agilizar numerosas actividades, también exponen a los usuarios a acciones delictivas que emplea para realizar fraudes y otros crímenes. Se entiende que el avance de la tecnología facilita el almacenamiento masivo de información en dispositivos digitales, lo que incrementa el riesgo de vulnerabilidades. En cuanto a Ecuador, el estudio destaca que, si bien el país ha dado pasos iniciales en la investigación y castigo por delitos cibernéticos, aún es necesario fortalecer y poner en marcha mecanismos regulados para mejorar la eficacia de dichas investigaciones.

b) Colombia. Moreno et al. (2022) realizó un estudio con el objetivo de analizar el delito de suplantación digital y proponer una regulación jurídica para garantizar el derecho humano a la identidad. La investigación utilizó los métodos sintéticos e inductivos, apoyándose en entrevistas a expertos en derecho tecnológico y penal. Los resultados revelaron que existe una regulación insuficiente o nula de este delito en muchos Estados, lo que preocupa especialmente ante el creciente uso de tecnologías en diversas actividades cotidianas. Los especialistas destacaron la necesidad urgente de tipificar este delito para proteger a los ciudadanos. Asimismo, concluyeron que aunque algunos países cuentan con regulaciones más avanzadas, es imprescindible promover una normativa global a través de tratados internacionales que permita enfrentar esta problemática de manera efectiva y coordinada.

Martínez (2022) llevó a cabo un estudio con enfoque cualitativo para analizar el impacto jurídico del delito de hurto informático en Colombia. La investigación evidencia que la legislación colombiana ha reconocido la necesidad de profundizar en aspectos tecnológicos,

dado que actualmente casi todas las actividades están sistematizadas. Sin embargo, el desarrollo normativo para prevenir y combatir este delito comenzó de manera tardía. No fue hasta 2011 que se creó una policía especializada en ciberdelitos, lo que ha dejado en desventaja a las autoridades frente a delincuentes con mayor experiencia en el uso de estas tecnologías. Esto plantea la urgencia de fortalecer las capacidades institucionales para enfrentar de manera efectiva este tipo de delitos en el país.

2.1.2 Antecedentes nacionales

En el Perú, de acuerdo a un reporte de la Defensoría del Pueblo (2023) respecto a la ciberseguridad, la suplantación de identidad representó el 20 % de los ciberdelitos denunciados ante la Policía Nacional en 2021. Se trata de uno de los delitos más recurrentes después del fraude informático, que afecta especialmente a personas y empresas que realizan transacciones en línea, así como a quienes desconocen el manejo y resguardo de sus datos personales. Aunque existen sanciones de hasta cinco años de encarcelamiento para este delito, su incidencia continúa en aumento debido a que los delincuentes emplean distintas tácticas para engañar a sus víctimas y acceder a su información personal (MPFN, 2024). Por citar algunos ejemplos ocurridos en nuestro país, tenemos los siguientes casos de estudio:

a) Lima. Monja (2022) investigó los delitos informáticos, centrando en la suplantación de identidad en entidades bancarias. Para tal fin se optó por un método básico y diseño no experimental. Entre sus hallazgos se pudo obtener que, pese a que los bancos cuentan con aparatos inteligentes para evitar fraudes y otros delitos, sigue sin ser suficiente. En conclusión, es necesario que se implementen nuevos métodos para detectar estos delitos a tiempo y que los culpables reciban condenas ejemplares debido a la magnitud del hecho.

Cervantes (2021) determinó la conexión entre la firma electrónica facial y el riesgo de suplantación de identidad en el centro de peritaje del Colegio de Ingenieros del Perú, Club Departamental de Lima. Por ello se decidió por un método correlacional y experimental, teniendo una población de 475 peritos y una muestra de 60. Entre sus hallazgos se obtuvo que las variables poseen una relación directa entre sí, llevando a concluir que los peritos deberían utilizar la firma electrónica en lugar de la tradicional, ya que esto evitaría casos de suplantación de identidad.

Aldecoa (2020) tuvo como propósito de la investigación analizar cómo los medios informáticos facilitan la suplantación de identidad, optando por un método cualitativo básico y de diseño interpretativo. Asimismo, tuvo una población de 2 abogados penalistas y 2 ingenieros. Entre sus resultados se obtuvo que no existen filtros adecuados para frenar este delito en la sociedad, y por ello se requiere de una mejor regulación y fiscalización. Se concluye que la suplantación de identidad es un delito que debe ser vigilado porque viene afectando a gran número de personas.

b) Chiclayo. Sandoval (2020) estableció los criterios necesarios para sancionar el delito de difamación por suplantación de identidad en Facebook. Por ello contó con un método cualitativo y diseño experimental, con una población de 102 operadores, entre jueces, fiscales y abogados. Sus resultados arrojaron que el 94 % de encuestados señalaron que es importante que este delito posea una sanción adecuada cuando se suplante la identidad de alguien en Facebook. Esto permitió concluir que el artículo 132 debe ser reformulado debido a que no es eficiente para establecer una sanción justa.

2.2. Bases teóricas

2.2.1 Medios informáticos

Los medios informáticos son herramientas o soportes que permiten a los individuos desarrollar diversas actividades, tales como la reproducción de datos, el manejo de material audiovisual, el entretenimiento, el esclarecimiento de hechos o el seguimiento de pericias, entre otros aportes valiosos, según las necesidades que presenten al hacer uso de estos (Romero García, 2021).

Como características de los medios informativos podemos encontrar que estas se pueden aplicar en distintas funciones prestando apoyo a la administración de justicia y la información judicial. Sin embargo, trae consigo nuevos problemas destacando el tema de validez y valoración de pruebas soportadas en medios informáticos. Asimismo, los medios informativos se pueden clasificar a su vez según su alcance en medios interpersonales que estén ligados a una comunicación más exhaustiva y privada, donde existe una cierta restricción en la información compartida debido a que no todas las personas tienen acceso a este. Por otro lado, tenemos los medios sociales, que son una información más general, la cual tiene como finalidad transmitir la información al mayor número de personas (Ibáñez P., 2020).

2.2.2 Dimensiones de Medios Informáticos

a) Soportes electrónicos. Son definidas como aquellas herramientas que permiten reproducir imágenes, videos, descifrar códigos, entre otras actividades. Son muy utilizadas porque permiten esclarecer los hechos y darles una certeza, sobre todo cuando se trata de casos de delitos o de la justicia. Los organismos federales distinguen a los delitos cibernéticos en tres grandes grupos. Sin embargo, en estos delitos es muy común que se use la computadora, ya que es aquí donde se roban datos, modifican usuarios y se transgrede la privacidad (Broadhurst, 2021).

Los soportes tecnológicos son mecanismos de control que proponen solución en dispositivos electrónicos con la finalidad de soportar las redes inteligentes que facilitan y hacen más flexible actuar frente a situaciones de investigación o de delitos mediante una base de datos que plantean desafíos en la seguridad de datos y legitimidad en derechos de autor (Ponce, 2024).

Si bien la tecnología ha brindado, como se mencionó, una serie de ventajas en los distintos sectores de la sociedad en el contexto de la educación, los docentes pueden aprovechar los recursos y brindar una enseñanza más eficiente y con mayor rapidez. Esto ha beneficiado a los estudiantes, quienes han sabido aprovechar esto. Sin embargo, las personas jóvenes, al no tener mayor conocimiento sobre los delitos de los cuales pueden ser víctimas, es necesario educarlos desde su primer contacto con estos medios, y así evitar fraudes, robos y otros hechos que les cause alguna perdida (Torres Flóres et al., 2022).

Los delitos cibernéticos que son cometidos a través de ordenadores son los más comunes. Pero independientemente del aparato que utilicen para cometerlo, en el hecho de amenazar, acosar o engañar a una persona ya se está incurriendo en un daño al individuo. En algunos casos existen razones grandes para regular estos delitos. Sin embargo, dependen netamente del país, las creencias y cómo este es tipificado en la ley (Mejía Lobo et al., 2023).

b) Formas de aportación de prueba. Son definidas como alternativas al momento de investigar un hecho en el cual se involucre un acto delictivo. Sirven como un aporte para entender el hecho y desenmascararlos ante la ley. Para tal fin son necesarias las pericias, pruebas indiciarias y otros mecanismos llevados a cabo por expertos (Ibáñez P., 2020). La forma de aportación se encuentra relacionado a las alternativas al momento de investigar un caso. Es decir, son herramientas que permiten esclarecer un hecho y que, a la vez, sirva como

apoyo. Para tal fin se recurre a las inspecciones judiciales, documentales o electrónicas. Cada uno de ellos pueden brindar credibilidad y certeza a los interesados (Ibáñez P., 2020).

c) Instrumentos de filmación. Los instrumentos de filmación son herramientas que favorecen a tener una visión clara de los hechos, los cuales son registrados en cámara o reproductores de cinta, con el objetivo de tener una comprensión y, a la vez, que sirva como medio de prueba ante algún delito. También son definidas como mecanismos que son usados en investigaciones de carácter penal porque ofrecen la reproducción de los hechos tal cual sucedieron en realidad. Asimismo, permiten perseguir actos ilícitos (Broadhurst, 2021).

2.2.3 Delito de suplantación de identidad

La suplantación de identidad es definida como un problema grave que cada vez se hace más común en la sociedad. Tiene como fin apropiarse de datos de una persona y usarlo para fines ilícitos. Esto se da con mayor razón en las redes sociales, ya que es aquí donde las personas pueden ser fácilmente engañadas. La ven como una ventaja, ya que pueden publicar o realizar comentarios sin que su nombre real se vea perjudicado. Es decir, participar de manera anónima en conversaciones reales. Sin embargo, también tiene su parte negativa porque debido a esto han aparecido los trolls y otros mecanismos para generar daño o perjudicar a ciertas personas (Dolores y otros, 2019).

Este tipo de delito es condenable dependiendo del daño causado y las circunstancias. Es decir, si hubo una ventaja económica, si se difundió prejuicios de una persona o si se vulneran los derechos del individuo (Arancibia, 2021). Este delito puede tener una pena de entre 1 a 3 meses o una prisión de 1 a 4 años. Cabrera et al. (2019) señalan que denunciar este crimen es sencillo siempre y cuando existan pruebas del hecho y se realice a tiempo. Con base a esto las autoridades actuarán y harán las diligencias del caso.

En el ordenamiento jurídico peruano, la Ley de Delitos Informáticos N° 30096, publicado el 22 de octubre de 2013, establece un marco legal para penalizar los delitos cometidos mediante el uso de tecnologías de la información. Esta norma tiene como objetivo regular el uso de los medios informáticos para prevenir, sancionar y erradicar los delitos digitales en el Perú (Huaroc, 2021).

En ese contexto, la Ley de Delitos Informáticos N° 30096 contempla una serie de delitos informáticos que permiten comprender cómo los medios digitales pueden ser utilizados como instrumentos para la comisión de ilícitos. Entre sus disposiciones más relevantes:

Artículo 2. Acceso ilícito: Sanciona el acceso no autorizado a computadoras, redes o bases de datos, lo cual puede ser el primer paso para obtener información privada con fines delictivos (Congreso de la República, 2013).

Posteriormente, la Ley N.º 30171, promulgada el 10 de marzo de 2014, amplió la definición, incluyendo el acceso que vulnera medidas de seguridad establecidas para impedirlo (Gobierno del Perú, 2024).

Como última modificación, en el 2023 mediante el Decreto Legislativo N.º 1614 se incrementó la pena a prisión no menor de tres ni mayor de seis años y multa de ochenta a ciento veinte días-multa para quien acceda vulnerando dichas medidas (Pasión por el derecho, 2024).

Artículo 3. Atentado contra la integridad de datos informáticos: Penaliza la interferencia o espionaje en la transmisión de datos, como la captura de contraseñas (Congreso de la República, 2013). La Ley N.º 30171 amplió el alcance de esta figura penal al incluir tanto la alteración ilegítima de datos como la incorporación de información falsa, fortaleciendo así las sanciones y abarcando un mayor número de conductas delictivas (Pasión por el derecho, 2024).

Artículo 4. Atentado contra la integridad de sistemas informáticos: Sanciona los actos que afectan el funcionamiento de sistemas informáticos, tales como ataques con virus o malware (Congreso de la República, 2013). La Ley N.º 30171 amplió los delitos informáticos, incluyendo no solo los daños a los sistemas, sino también las acciones que dificultan o impiden su acceso. Además, aumentó las penas, estableciendo una prisión de entre tres y seis años y una multa de ochenta a ciento veinte días-multa (Pasión por el derecho, 2024).

Si bien estas figuras jurídicas se orientan a sancionar ataques directos a la infraestructura digital o a los datos que en ella circulan, también permiten visibilizar cómo dichos actos pueden ser el punto de partida para la planificación o ejecución de delitos más elaborados y personalizados, como es el caso de la suplantación de identidad, en los que el acceso, manipulación o control indebido de información se convierte en un recurso clave para generar perjuicio:

Artículo 9. Suplantación de identidad: Toda persona que utilice medios digitales para hacerse pasar de manera ilegítima por otra, ya sea una persona física o una entidad jurídica, cuya acción cause algún tipo de daño ya sea económico, moral o de otra naturaleza, será sancionada con una pena de prisión que no podrá ser menor de tres años ni exceder los cinco años (Congreso de la República, 2013).

A través del Decreto Legislativo Nº 1591, emitido el 13 de diciembre de 2023, se introdujeron modificaciones en la normativa correspondiente, reemplazándose la expresión relacionada con “Tecnologías informáticas” por una que alude a “Tecnologías digitales” y además se incorporó una disposición específica que incrementa la sanción penal, estableciendo que si la identidad falsificada corresponde a un menor de edad y se produce algún tipo de daño, la condena oscila entre seis y nueve años de privación de libertad (Gobierno del Perú, 2023).

Phishing. Este delito consiste en enviar correos electrónicos engañosos o crear páginas fraudulentas que perjudiquen el tráfico de datos personales de un usuario, así como la manipulación financiera. Además, busca vulnerar la seguridad sistemática y acceder a contraseñas personales para llevar a cabo hechos delictivos. Solo tiene éxito cuando los delincuentes atraen a usuarios a través de mentiras o amenazas para apoderarse de sus datos. Estas técnicas de manipulación casi siempre se dan porque las personas no leen detenidamente a donde acceden o carecen la información necesaria, siendo impulsivos, sobre todo cuando se les promete alguna ganancia económica (Ahmad, 2020).

A continuación, se presenta una comparación entre países que han sufrido casos de este delito:

Según Kulikova et al. (2021), en primer lugar, se encuentra México, estando en la cima de los países latinoamericanos que contantemente reciben correos electrónicos maliciosos (incluidos archivos o enlaces), evidenciado en un 3.34 %. En cuanto a los países de nivel regional, tenemos a Brasil, con un 3.33 %, convirtiéndose en el país de Sudamérica más afectado, seguido por Colombia con un 0.87 % y Perú con un 0.63 %. Respecto a Europa, tenemos a España en un 8.48 %, Alemania en 7.05 % y Rusia en 5.87 %.

Volviendo a Brasil, este país durante el año 2020 registró un sistema de anti-phishing, neutralizando 434.898.635, plataforma que redirigió a los usuarios de sistemas maliciosos, sin embargo, esto no evitó que los casos se siguieran cometiendo, evidenciado en un 19.94 %. Portugal ocupa el segundo lugar con un 19.73 %, Francia con un 17.90 % (Kulikova et al., 2021).

2.2.4 Dimensiones de infracciones de suplantación de identidad

Apropiación de datos por medios convencionales o informáticos. Se refiere a la suplantación de identidad de una persona, realizado para obtener algún provecho, los expertos

en el tema señalan que este delito es uno de los más graves porque afecta a la persona de forma directa, haciendo que esta pierda contraseñas importantes, afectando su estado financiero o económico (Mayer & Oliver, 2020).

Los programadores o editores de código brindan las herramientas necesarias para que los usuarios puedan conocer cuando algún enlace, correo o página web es fraudulento. Sin embargo, hoy en día existen tantos delitos que buscan obtener un intercambio monetario que las herramientas de seguridad son cada vez más insuficientes (Aparicio, 2018).

El software malicioso o también llamado "malware" es un sistema que busca capturar a los usuarios, adoptando formas de virus, gusanos troyanos o algunos otros, son difíciles de eliminar del ordenador una vez que están dentro, incluso para las víctimas resulta costoso. El exploit es un sistema que engaña a las personas para que este descargue contenido y así realizar cambios internos en el ordenador, capturando contraseñas, datos o información importante. Sin embargo, también daña archivos y accede a información privada (Broadhurst, 2021).

Además, es importante señalar que las personas en su momento de diversión o de locura acceden a paginas fraudulentas por propia decisión, ya sea para jugar una broma o para saber qué es lo que hay ahí, siendo este contenido ilícito y penado (Vásquez y otros, 2020).

Transferencia o cesión de datos personales. Se define como aquella revelación de datos que posee una persona, pero que se da por un tercero, siendo un proceso extenso que posee ciertos pasos para que estos lleguen a un destinario. Es un mecanismo que brinda información de un usuario. Para llevar a cabo este proceso es necesario contar con el permiso de la persona y del usuario que posee la data. Sin embargo, hoy en día se da a cambio de un beneficio económico, siendo penado por ley. Los delincuentes que cometen este delito comprometen sistemas legítimos para alojar sus sitios, los archivos o data solo se carga a la

web, aprovechando que este posee una seguridad baja. Las técnicas típicas para cometer este delito son los foros que poseen imágenes, carrito de compras, blogs, llenado automático, parches correctivos, entre otros (Rivera Barrantes, 2019).

Utilización de datos personales. Existen diversas formas para que los datos puedan ser robados. Esto otorga una ventaja a quien lo posea, y en afán de aprovecharse de esto y perjudicar a la persona, los delincuentes son muy creativos para usarlos**.** La utilización de datos sea en su mayoría por robos, donde los delincuentes buscan obtener alguna ganancia, por lo que no les importa si amenazan, mienten o sobornan a la persona para que en base a sus peticiones logren su cometido (Ojeda & Cutié, 2022).

2.3. Definición de términos básicos

Tabla 1

Definición de términos

Términos básicos	Definición
Apropiamiento de soportes lógicos	Es un elemento intangible que se encuentra en las bases de datos automáticas, sirviendo como soportes de materiales (García, 2020).
Archivos	Son aquellos documentos que se encuentran clasificados de forma ordenada, es información confidencial de cada entidad o personas (Fernández & Sanz, 2021).
Cámaras de videovigilancia	Son aparatos tecnológicos que permiten monitorear y supervisar cualquier actividad que pueda suceder en un lugar determinado (Rodríguez, 2018).

Comercialización previa de grandes bases de datos de personas	Son información importante sobre posibles consumidores o usuarios, en marketing esta es una herramienta importante (Marcos Ayjón, 2020).
Cualidades atributivas y racionales con el ente de imputación jurídica	Se refieren a un condición o facultad para acceder o hacer uso de datos de forma ilícita (Benavente Chorres, 2021).
Datos obtenidos de manera ilícita	Se trata de información de clientes o usuarios que han sido obtenidos a cambio de un pago ilegal o sin el consentimiento de estos (Estévez, 2019).
Experticia o pericia	Es una ciencia que permite aceptar o rechazar una hipótesis (Piva y otros, 2021).
Inspección judicial	Es una evaluación que consiste en investigar el estado de una persona (Aranda, 2021).
Producción de actos o consecuencias legales	Se refiere a la existencia de leyes que protejan a los ciudadanos y los obligue a vivir plenamente en sociedad (González, 2021).
Prueba iniciaría	Es un documento que reúne acontecimientos que se han realizado, el fin es verificarlos y dar fe que en realidad sí sucedieron (Dellepiane, 2021).
Reproducción de datos	Es una reproducción de información para fines investigativos (Fernández & Sanz, 2021).
Reproductores de cintas magnetofónicas	Es un tipo de soporte que tiene la capacidad de almacenar información, grabando los datos en una banda plástica (Tenorio & López, 2021).

Signos, símbolos o códigos	Son imágenes que representa algún significado para quien lo lee, existe una gran variedad hoy en día (Piva y otros, 2021).
Usurpación de bienes incorpóreos	Es aquel delito que busca recopilar información de un individuo y usarlo para fines malignos (Avendaño & Avendaño, 2017).

CAPÍTULO III

HIPÓTESIS Y VARIABLES

3.1. Hipótesis

3.1.1. Hipótesis General

- Los medios informáticos influyen significativamente en el delito de suplantación de identidad, Lima, periodo 2023-2024.

3.1.2. Hipótesis Específicas

- Los medios informáticos influyen significativamente en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.

- Los medios informáticos influyen significativamente en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.

- Los medios informáticos influyen significativamente en la utilización de datos personales, Lima, periodo 2023-2024.

3.2. Variables de Estudio

3.2.1 Variable independiente

Medios informáticos

3.2.2 Variable dependiente

Suplantación de identidad

CAPÍTULO IV

METODOLOGÍA

4.1. Tipo de diseño y alcance de la investigación

4.1.1. Tipo de diseño de la investigación

La investigación fue de tipo básico, ya que se orientó a profundizar en el conforme a nuestra legislación penal vigente de los resultados. Este tipo de investigación se caracteriza por generar nuevos saberes desde una perspectiva fundamental, centrada en la comprensión y explicación de fenómenos, con el objetivo de ampliar el cuerpo teórico existente en un determinado campo del conocimiento (Concepción y otros, 2019).

4.1.2. Alcance de la investigación

El alcance fue descriptivo, puesto que se centró en identificar y detallar las características del delito de suplantación de identidad a través de los medios informáticos en Lima, durante el periodo 2023-2024, permitiendo observar y representar la realidad tal como se presenta, ampliando la comprensión del fenómeno sin intervenir o modificar sus variables. Según Gallardo (2017), esta elección permite describir la realidad y ampliar la información que existe sobre ella, de manera que con los datos que se obtengan se pueda evidenciar nuevas conclusiones y recomendaciones para su solución.

Además, el diseño fue no experimental-transeccional, el cual consiste en analizar el fenómeno de estudio sin la necesidad de manipular las variables durante el proceso. Es decir, solo se practica la observación, descripción e interpretación de los resultados (Niño, 2021).

Finalmente, este estudio fue de carácter jurídico-descriptivo, el cual buscó desglosar el fenómeno de estudio para poder analizarlo de forma sencilla.

4.2. Enfoque de la investigación

El enfoque de la investigación fue cuantitativo porque se requería medir y analizar el impacto de los medios informáticos en el delito de suplantación de identidad a través de una recopilación precisa de información mediante encuestas y otras técnicas que brindaron datos estadísticos claros, los cuales son necesarios para comprender la magnitud del fenómeno. De acuerdo con Hernández et al. (2014), dicho enfoque permite recopilar una vasta información, a partir de datos numéricos, frecuencias, datos porcentuales y desarrollo de procesos estadísticos que permitan la correcta medicación de las variables.

4.3. Horizonte temporal

4.3.1 Horizonte espacial

Esta investigación esta llevada a cabo en la DIRINCRI, ubicada en la ciudad de Lima.

4.3.2 Horizonte social

Se busca determinar cómo el uso de los medios informáticos influye en el delito de suplantación de identidad, periodo 2023-2024. Esto para que las autoridades y la ciudadanía tomen conciencia de que el delito viene cobrando relevancia y causando gran daño.

4.3.3 Horizonte tiempo

Toda la presente investigación fue desarrollada en el año 2023- 2024

4.4. Población y Muestra

4.4.1 Población

La población es un conjunto masivo de personas que entre sí poseen características similares, y por ello pueden ser analizados respecto a un mismo fenómeno que les afecte (Ventura, 2017).

En este estudio la población fueron 128 efectivos policiales de la DIRINCRI y las denuncias DIVINDAT 2023-2024 por el delito contra la fe pública, modalidad de suplantación de identidad.

4.4.2 Muestra

La muestra es un subconjunto de personas extraídas de la población, quienes, al ser un número reducido de personas, el análisis puede ser llevado a cabo de forma más rápida y sencilla en beneficio del estudio (Ventura, 2017).

La muestra fue de 25 efectivos de la DIRINCRI especialistas en el área de delitos informáticos y las denuncias DIVINDAT 2023-2024 por el delito contra la fe pública, modalidad de suplantación de identidad.

4.5. Recolección de datos

Para la recolección de información en esta investigación, se utilizó la encuesta, ya que resulta una herramienta apropiada para obtener datos específicos y cuantificables en un grupo especializado, como en el caso de los efectivos de la DIRINCRI. De acuerdo con Arias (2021), la encuesta es una herramienta útil para ser aplicada a grupos específicos, permitiendo la recolección de información sobre opiniones, experiencias y percepciones a través de preguntas estructuradas. Esta técnica resulta especialmente adecuada cuando se busca obtener datos detallados y cuantificables.

Como instrumento de recolección se desarrolló el cuestionario, siendo una herramienta muy sencilla de aplicar debido a que establece un conjunto de preguntas estructuradas y coherentes al tema de investigación, el cual fue aplicado a la muestra de estudio, quienes dieron respuesta siguiendo la escala de Likert. Según Medina et al. (2023) este instrumento permite recolectar datos relevantes y organizados de una muestra determinada en relación con una

temática específica, a través de una estructura compuesta por ítems de tipo dicotómico, politómico o fundamentados en escalas.

Por otro lado, se adoptó la técnica de observación, la cual permitió recolectar información actual y real del fenómeno de estudio sin influir en el contexto en el que se desarrollan los hechos. Tal y como señala Arias (2021), la observación es una técnica donde el investigador observa de forma sistemática sin intervenir en el entorno, manteniendo una postura externa y neutral durante el proceso, cuyo propósito es evitar influencias que alteren el comportamiento natural de los sujetos.

Adicionalmente, se empleó la ficha de observación que permitió recolectar datos sistemáticos sobre las denuncias de suplantación de identidad y las pérdidas económicas asociadas. Permite obtener información objetiva y comparable, facilitando un análisis riguroso de la magnitud del delito. Esto concuerda con Medina et al. (2023) quienes afirman que la ficha de observación es un instrumento que registra de manera sistemática y objetiva comportamientos, acciones o características de un sujeto o fenómeno, cuya correcta elaboración minimiza el sesgo y facilita el análisis comparativo de la información.

Es importante señalar que para la realización de este estudio se respetó la integridad científica, a través de los procedimientos y técnicas respaldas por autores. Es decir, se llevó a cabo una investigación responsable e imparcial, donde no se favoreció a nadie y la recolección de data se dio a través de métodos confiables y trasparentes, bajo fines 100 % académicos (Reyes, 2018).

4.5.1 Validez de los instrumentos

Tabla 2

Validez de los instrumentos

Experto	Apellidos y nombres	Grado académico	Resultado
Experto 01	Guerrero Muñoz, Rody Aníbal	Maestro	Aplicable
Experto 02	Santamaría Portocarrero Walter	Maestro	Aplicable
Experto 03	Salazar Llerena, Silvia Liliana	Doctora	Aplicable

Para determinar la validez del instrumento, se recurrió al juicio de expertos, quienes evaluaron su pertinencia, coherencia y adecuación en relación con los objetivos y variables del estudio. En esta etapa participaron tres especialistas con grado académico de maestría y doctorado, cuyos aportes permitieron verificar la validez de contenido del instrumento. Tal como se muestra en la Tabla 2, los expertos Rody Aníbal Guerrero Muñoz, Walter Santamaría Portocarrero y Silvia Liliana Salazar Llerena coincidieron en calificar el instrumento como aplicable, lo que respalda su uso en el proceso de recolección de datos para la presente investigación.

4.5.2 Confiabilidad del instrumento

Tabla 3

Confiabilidad

Variables	Alfa de Cronbach	N de elementos
Medios informáticos	0.828	16
Delito de suplantación de identidad	0.837	12

Por medio del alfa de Cronbach, se evidenció que el valor de la variable "Medios informáticos" es de 0,828; mientras que para la segunda variable hay un 0,837, considerado ambos como aceptables y fiables para su utilización dentro de la investigación. Se garantiza así que los datos obtenidos mediante el cuestionario aplicado a los 25 efectivos de la DIRINCRI, especializados en delitos informáticos, sean consistentes y reflejen de manera estable las percepciones y experiencias recogidas. Esto resulta fundamental para respaldar la solidez de los datos obtenidos en el estudio, ya que permite contar con una base estadísticamente fiable sobre la cual analizar la relación entre el uso de medios informáticos y el delito de suplantación de identidad en Lima, durante el periodo 2023-2024.

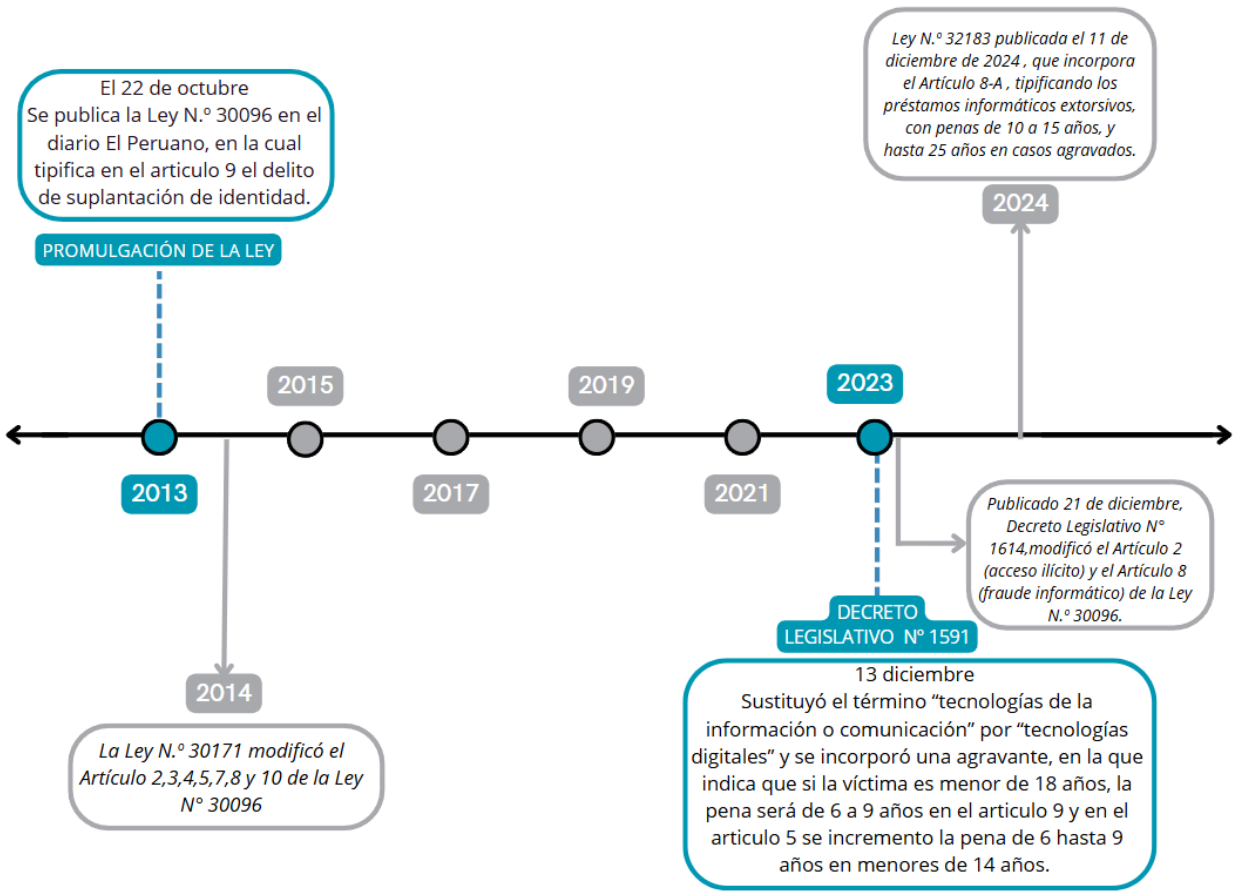
CAPÍTULO V

RESULTADOS Y DISCUSIÓN

5.1. Resultados

Figura 1

Evolución normativa sobre delitos informáticos y suplantación de identidad en Perú



Esta línea de tiempo muestra la evolución normativa sobre delitos informáticos y suplantación de identidad en Perú. Destaca como tema principal su inclusión en la Ley N.º 30096, publicada en el año 2013, que es un avance significativo, ya que en dicho año se tipificó oficialmente el delito de suplantación de identidad, el cual se convirtió en una figura penal dentro del marco de la ciberdelincuencia. A partir de esta modificación, el Código Penal comenzó a considerar este tipo de ilícito con penas que oscilan entre 3 y 5 años de prisión,

marcando el inicio de un enfoque jurídico más riguroso para enfrentar los delitos informáticos en el Perú.

El cambio más reciente en torno al delito de suplantación de identidad se produjo en el año 2023, con una reforma que introdujo un agravante significativo: si la víctima del delito es un menor de edad, la pena puede incrementarse, alcanzando un rango de 6 a 9 años de prisión. Este cambio refleja un endurecimiento de las sanciones y una mayor protección hacia los sectores más vulnerables de la sociedad, como los menores de edad, quienes se ven especialmente expuestos a los riesgos asociados con la suplantación de identidad a través de medios digitales.

Un primer hito complementario ocurrió en 2014, con la publicación de la Ley N.º 30171. Esta ley modificó varios artículos de la Ley N.º 30096, incluyendo los artículos 2, 3, 4, 5, 7, 8 y 10, ampliando el enfoque penal para abordar otros delitos informáticos de relevancia, como el acceso no autorizado a sistemas informáticos, el atentado contra la integridad de datos y sistemas informáticos, y el fraude informático. Estas modificaciones fortalecieron la lucha contra diversos tipos de ciberdelincuencia, incorporando nuevas conductas punibles como el acceso que vulnera medidas de seguridad establecidas para impedirlo, y ajustando las penas para hacer frente a la creciente sofisticación de estos delitos, creando un marco normativo más robusto para la protección de la información y los sistemas digitales.

Por consiguiente, esta línea de tiempo refleja cómo las modificaciones legales han ido evolucionando para abordar el delito de suplantación de identidad, con una especial atención a la inclusión de agravantes y al fortalecimiento de las penas. Además, se observa cómo las reformas complementarias relacionadas con otros delitos informáticos han servido para ampliar el marco de protección contra la ciberdelincuencia en el Perú, contribuyendo a la creación de un sistema normativo más integral en este campo.

En la presente investigación se desarrolló una ficha de observación, la cual, de acuerdo con Menchú (2017), tiene relación a cuando el investigador quiere medir, analizar o evaluar un objetivo en específico. Por otro lado, mediante el análisis documental se buscó examinar a profundidad los datos, con la intención de llegar a saber sus elementos principales y, por ende, la relación que guardan entre ellos (Marcelino et al., 2024).

Tabla 4

Ficha de observación

FICHA DE OBSERVACIÓN	
Nombre del documento	Denuncias DIVINDAT 2023-2024 por el delito contra la fe pública, modalidad de suplantación de identidad
Autor	División de Investigación de Delitos de Alta Tecnología.
Dirección electrónica de la entidad de información	https://www.policia.gob.pe/
Palabra claves del texto	Denuncias, pérdidas económicas y suplantación de identidad.
Descripción del aporte al tema seleccionado	El aporte a la investigación es el que da a conocer la cantidad de denuncias y pérdidas precisadas por las víctimas mensualmente durante el periodo 2020 – 2021, por el delito contra la fe pública, modalidad de suplantación de identidad.
Conceptos abordados	- Denuncias mensuales. - Suma de denuncias anual. - Pérdidas mensuales. - Suma de pérdidas anual.
Objetivo del análisis	Como parte de los objetivos, se precisa dar a conocer cuántas denuncias se han tenido mensualmente durante el 2023 y 2024, junto a la sumatoria anual de cada uno de esos años. De la misma manera, hacerlo también con las pérdidas económicas que tuvieron las víctimas en dicho periodo, midiendo así la magnitud del delito.

Tabla 5

Denuncias DIVINDAT por el delito contra la fe pública, modalidad de suplantación de identidad en números ordinales - año 2023

MES/AÑO: 2023	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre	TOTAL	%
Denuncias	245	205	180	120	135	320	370	355	380	440	491	543	3784	**100%**
Pérdida en soles	S/ 524,152.56	S/ 432,524.54	S/ 320,160.10	S/ 230,546.00	S/ 320,338.00	S/ 860,832.00	S/ 1,210,765.00	S/ 1,115,600.00	S/ 1,133,751.00	S/ 1,298,645.00	S/ 1,345,873.00	S/ 1,480,645.00	S/ 10,273,832.20	**100%**

Fuente: Denuncias DIVINDAT. (2023)

Interpretación:

Respecto a las denuncias que se interpusieron y las pérdidas soles que se produjeron en la DIVINDAT referidas al delito contra la fe pública en la modalidad de suplantación de identidad en el año 2023, se determinó lo siguiente: el mes de mayor número de denuncias se encontró en diciembre, con un total de 543 denuncias. De la misma forma, el mes con menos número de denuncias se encontró en el mes de abril, con un total de 120 denuncias. De lo anterior cabe decir que la mayor concentración se encuentra cerca a los mese donde se realizan días festivos, como en este caso la Navidad.

Tabla 6

Denuncias DIVINDAT por el delito contra la fe pública, modalidad de suplantación de identidad en porcentajes - año 2023

MES/AÑO: 2023	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre	TOTAL	Nro.
Denuncias	6.47 %	5.42 %	4.76 %	3.17 %	3.57 %	8.46 %	9.78 %	9.38 %	10.04 %	11.63 %	12.98 %	14.35 %	**100 %**	**3784**
Pérdida en soles	5.10 %	4.21 %	3.12 %	2.24 %	3.12 %	8.38 %	11.78%	10.86%	11.04 %	12.64 %	13.10 %	14.41 %	**100 %**	**S/ 10,273,832.20**

Fuente: Denuncias DIVINDAT. (2023)

Interpretación:

Respecto a la cantidad en porcentaje de denuncias y pérdidas que se produjeron en la DIVINDAT, referidas al delito contra la fe pública en la modalidad de suplantación de identidad en el año 2023, se determinó lo siguiente: el mes de mayor índice delictivo se encontró en diciembre, con un total de 14.35 % de denuncias. De la misma forma, el mes con menos índice delictivo se encontró en el mes de abril, con un total de 3.17 % de denuncias. De lo anterior cabe decir que en los días festivos como en Navidad se concentra el mayor índice delictivo, lo cual resulta perjudicial para la entidad.

Tabla 7

Denuncias DIVINDAT por el delito contra la fe pública, modalidad de suplantación de identidad en números ordinales - año 2024

MES/AÑO: 2024	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre	TOTAL	%
Denuncias	250	278	224	190	208	224	305	293	264	273	260	289	**3058**	**100%**
Pérdida en soles	S/ 811,370.00	S/ 860,487.00	S/ 828,370.65	S/ 710,450.00	S/ 1,220,929.50	S/ 1,227,171.00	S/ 1,430,100.00	S/ 1,395,276.61	S/ 1,271,041.77	S/ 1,212,800.00	S/ 1,177,379.00	S/ 1,327,780.15	**S/ 13,473,155.68**	**100%**

Fuente: Denuncias DIVINDAT (2024)

Interpretación:

Respecto a las denuncias que se interpusieron y las pérdidas en soles que se produjeron en la DIVINDAT referidas al delito contra la fe pública en la modalidad de suplantación de identidad en el año 2024, se determinó lo siguiente: el mes de mayor índice delictivo se encontró en julio, con un total de 305 denuncias. De la misma forma, el mes con menos índice delictivo se encontró en el mes de abril, con un total de 190 denuncias. De lo anterior cabe decir que se sigue manteniendo que en los meses donde se encuentran días festivos como el Día de la Independencia del Perú, como también un mes posterior a estos, se muestran que incrementa el índice de denuncias. Por otro lado, comparando el número total de denuncias del año anterior con el siguiente se puede observar que existe una disminución en el índice delictivo.

Tabla 8

Denuncias DIVINDAT *por el delito contra la fe pública, modalidad de suplantación de identidad en porcentajes - año 2024*

MES/AÑO: 2024	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre	TOTAL	Nro.
Denuncias	8.18 %	9.09 %	7.33 %	6.21 %	6.80 %	7.33 %	9.97 %	9.58 %	8.63 %	8.93 %	8.50 %	9.45 %	**100**	**3058**
Pérdida en soles	6.02 %	6.39 %	6.15 %	5.27 %	9.06 %	9.11 %	10.61 %	10.36 %	9.43 %	9.00 %	8.74 %	9.86 %	**100**	**S/ 13,473,155.68**

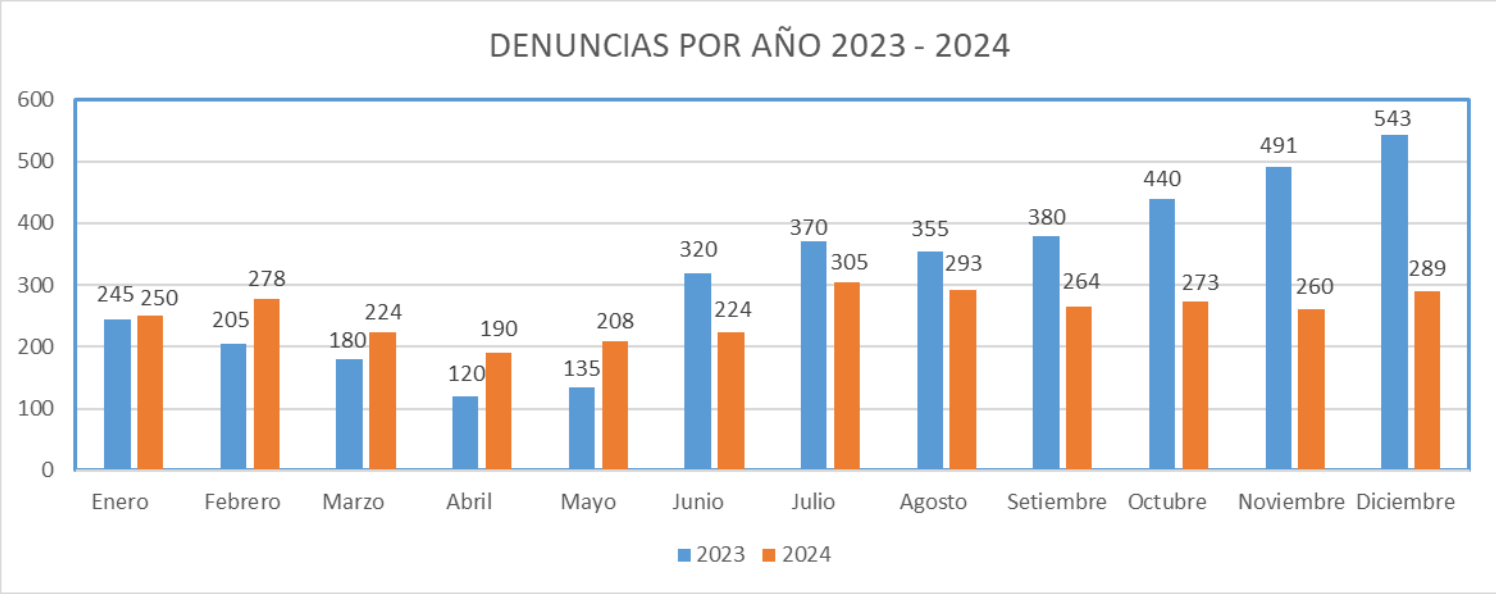
Fuente: Denuncias DIVINDAT. (2024)

Interpretación:

Respecto a las denuncias que se interpusieron y las pérdidas en soles que se produjeron en la DIVINDAT referidas al delito contra la fe pública en la modalidad de suplantación de identidad en el año 2024, se determinó lo siguiente: el mes de mayor índice delictivo se encontró en julio, con un total de 9.97 % de denuncias. De la misma forma, el mes con menos índice delictivo se encontró en el mes de abril, con un total de 6.21 % de denuncias. De lo anterior cabe decir que se sigue manteniendo que en los meses donde se encuentran días festivos, como también un mes posterior a estos, se muestra un aumento del índice delictivo.

Figura 2:

Comparativa de cantidad de denuncias mensuales durante el 2023 - 2024

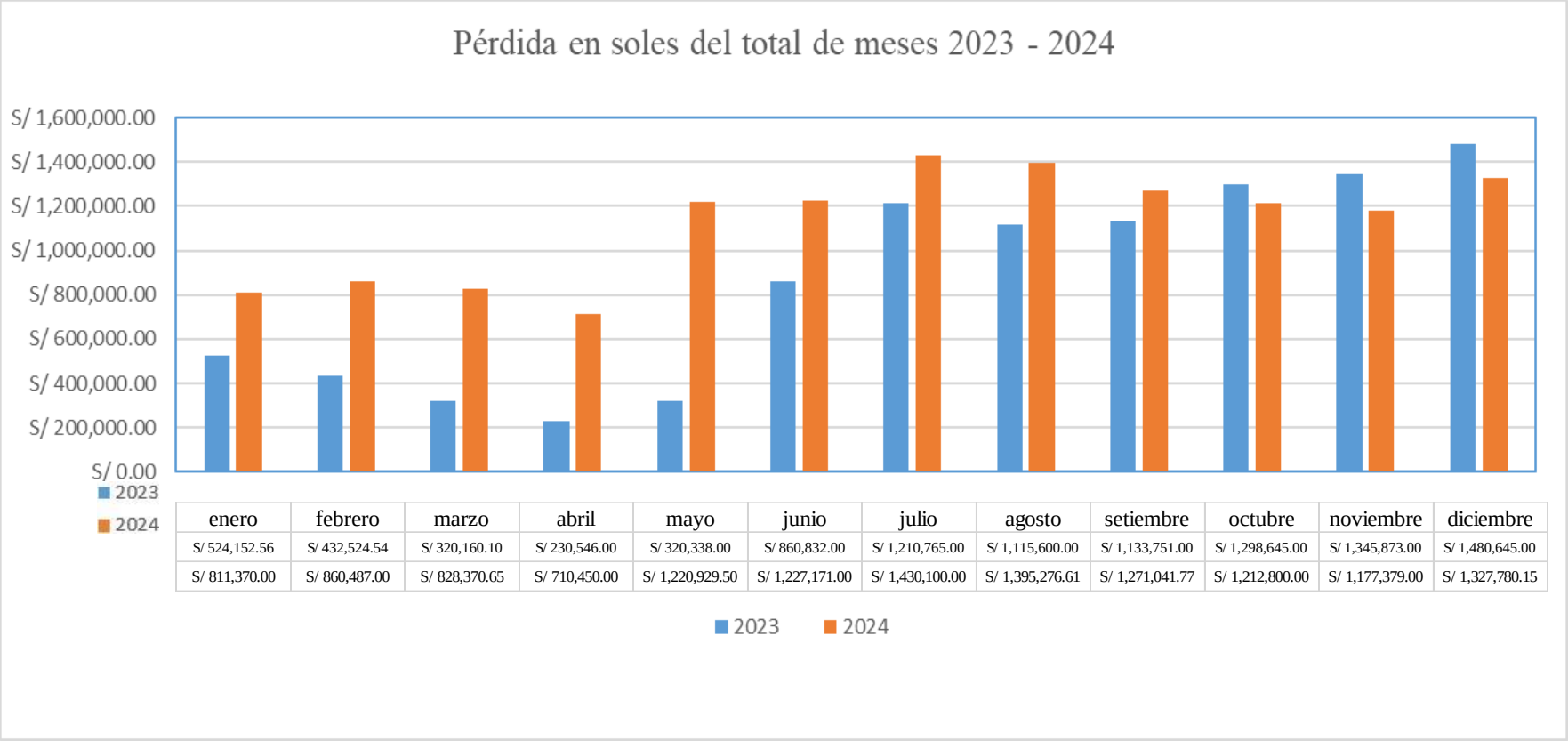


Interpretación:

De acuerdo con la figura 2, se aprecia los casos reportados entre el año 2023 - 2024, en la cual se verifica una diferencia que dista en 726, puesto que en el 2023 se reportaron 3784 casos y en el 2024, 3058 casos.

Figura 3:

Comparativa de pérdidas económicas mensuales durante el 2023 - 2024



Interpretación:

De acuerdo con la figura 3, se aprecia que las pérdidas económicas en el año 2023 tienen un índice mayor en los meses de diciembre y noviembre. Asimismo, en el año 2024 se tiene que los índices más crecientes se establecieron en los meses de julio, agosto y diciembre, donde se verifica que dentro del año 2024 se establecieron mayores pérdidas que en el año 2023. Además, comparando los meses de ambos años se puede decir que donde el año anterior hubo menores pérdidas y en el siguiente año se aumentó considerablemente. Analizando ambos años, se encontró una diferencia que dista en S/ 3,199,323.48, puesto que en el 2023 se reportaron S/ 10,273,832.20; y en el 2024, S/ 13,473,155.68.

5.1.1. Análisis descriptivo

a) Niveles y rangos de la variable medios informáticos.

Tabla 9

Niveles y rangos de la variable medios informáticos

Nivel	Rango
Bajo	16 - 37
Medio	38 - 59
Alto	60 - 80

b) Resultados obtenidos de la encuesta: variable medios informáticos.

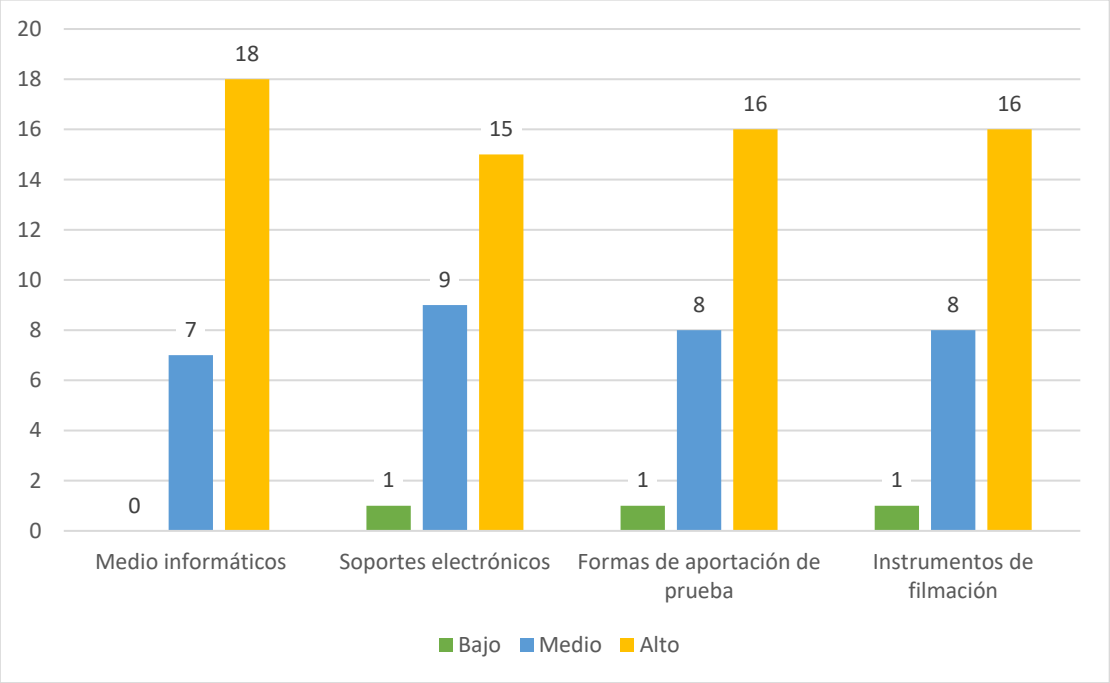
Tabla 10

Análisis descriptivo de la variable medios informáticos

		V1: Medios informáticos		D1: Soportes electrónicos		D2: Formas de aportación de prueba		D3: Instrumentos de filmación	
		f_i	h_i	f_i	h_i	f_i	h_i	f_i	h_i
Válido	Bajo	0	0,0 %	1	4,0 %	1	4,0 %	1	4,0 %
	Medio	7	28,0 %	9	36,0 %	8	32,0 %	8	32,0 %
	Alto	18	72,0 %	15	60,0 %	16	64,0 %	16	64,0 %
	Total	25	100,0 %	25	100,0 %	25	10,00 %	25	100,0 %

Figura 4

Análisis descriptivo de la variable medios informáticos.



Referente a la variable “Medios informáticos”, se evidenció que 7 de los encuestados reflejaron que se encuentran en un nivel medio y unos 18 en un nivel alto. Continuando con la dimensión “soportes electrónicos”, se pudo evidenciar que 1 de los encuestados la consideró en un nivel bajo, 9 de ellos en un nivel medio y 15 de ellos en un nivel alto. Continuando con la dimensión “Formas de aportación de prueba”, se demostró que 1 de los encuestados la consideró en un nivel bajo, 8 de ellos en un nivel medio y por último 16 de ellos en un nivel alto. Finalmente, dentro de la dimensión “Instrumentos de filmación” se pudo demostrar que 1 de los encuestados la considera en un nivel bajo, 8 de ellos en un nivel medio y por último 16 de ellos en un nivel alto.

c) Niveles y rangos de la variable Delito de suplantación de la identidad

Tabla 11

Niveles y rangos de la variable delito de suplantación de la identidad

Nivel	Rango
Bajo	12 – 28
Medio	29 - 45
Alto	46 - 60

d) Resultados obtenidos de la encuesta: variable Delito de suplantación de la identidad

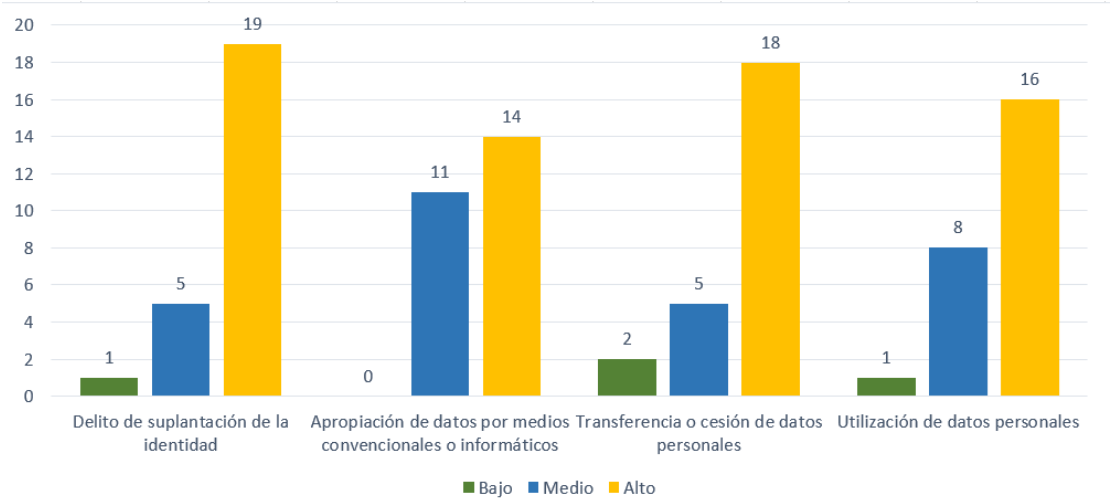
Tabla 12

Análisis descriptivo de la variable delito de suplantación de la identidad y sus dimensiones

		V1: Delito de suplantación de la identidad		D1: Apropiación de datos por medios convencionales o informáticos		D2: Transferencia o cesión de datos personales		D3: Utilización de datos personales	
		f_i	h_i	f_i	h_i	f_i	h_i	f_i	h_i
Válido	Bajo	1	4,0 %	0	0,0 %	2	8,0 %	1	4,0 %
	Medio	5	20,0 %	11	44,0 %	5	20,0 %	8	32,0 %
	Alto	19	76,0 %	14	56,0 %	18	72,0 %	16	64,0 %
	Total	25	100,0 %	25	100,0 %	25	100,0 %	25	100,0 %

Figura 5

Análisis descriptivo de la variable delito de suplantación de la identidad y sus dimensiones



Referente a la variable "Delito de suplantación de la identidad", se evidenció que 1 de los encuestados reflejó que se encuentra en un nivel bajo, 5 de ellos la consideraron en un nivel medio y unos 5 en un nivel alto. Continuando con la dimensión "Apropiación de datos por medios convencionales o informáticos", se pudo evidenciar que 11 de los encuestados la consideraron en un nivel bajo, 14 de ellos en un nivel medio y 25 de ellos en un nivel alto. Continuando con la dimensión "Transferencia o cesión de datos personales", se demostró que 2 de los encuestados la consideró en un nivel bajo, 5 de ellos en un nivel medio y por último 18 de ellos en un nivel alto. Finalmente, dentro de la dimensión "Utilización de datos personales" se pudo demostrar que 1 de los encuestados la considera en un nivel bajo, 8 de ellos en un nivel medio y por último 16 de ellos en un nivel alto.

5.1.2. Análisis inferencial

a) Hipótesis general

H1: Los medios informáticos influyen significativamente en el delito de suplantación de identidad, Lima, periodo 2023-2024.

H0: Los medios informáticos no influyen significativamente en el delito de suplantación de identidad, Lima, periodo 2023-2024.

Tabla 13

Correlación entre las variables medios informáticos y el delito de suplantación de identidad.

		Medios informáticos	Delito de suplantación de identidad
Medios informáticos	Correlación de Pearson	1	,808**
	Sig. (bilateral)		,000
	N	25	25
Delito de suplantación de identidad	Correlación de Pearson	,808**	1
	Sig. (bilateral)	,000	
	N	25	25

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

La Tabla 13 evidencia una correlación positiva alta con un coeficiente de Pearson r=0.808 y un nivel de significancia de p=0.00, inferior al umbral establecido en 0.05. Estos resultados permiten rechazar la hipótesis nula, y confirman que los medios informáticos influyen significativamente en el delito de suplantación de identidad, Lima, periodo 2023-2024. Estos hallazgos muestran la necesidad de fortalecer las medidas de ciberseguridad y la protección de datos personales en entornos digitales.

Tabla 14

Resumen del modelo 1

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	,808[a]	,654	,639	4,746

La Tabla 14 presenta un coeficiente de determinación (R^2) de 0,654, lo que indica que el 65,4 % de la variabilidad observada en el delito de suplantación de identidad puede ser

explicada por el uso o disponibilidad de medios informáticos. Es decir, a medida que se intensifica el uso de estos recursos tecnológicos, también tiende a incrementarse la incidencia de dicho delito. Este resultado sugiere que los medios informáticos ejercen una influencia significativa en la ocurrencia del delito analizado, por lo que deben considerarse como un elemento clave en el diseño de estrategias preventivas, normativas de control y políticas públicas orientadas a mitigar los delitos cibernéticos.

Tabla 15

ANOVA - Modelo 1

Modelo 1	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	977,444	1	977,444	43,400	,000[b]
Residuo	517,996	23	22,522		
Total	1495,440	24			

La Tabla 15 muestra los resultados del análisis ANOVA, donde se evidencia que el modelo 1 presenta un nivel de significancia inferior a 0.05, lo cual demuestra que existe sustento estadístico para establecer un modelo de regresión lineal entre las variables Medios Informáticos y Delito de Suplantación de Identidad.

Tabla 16

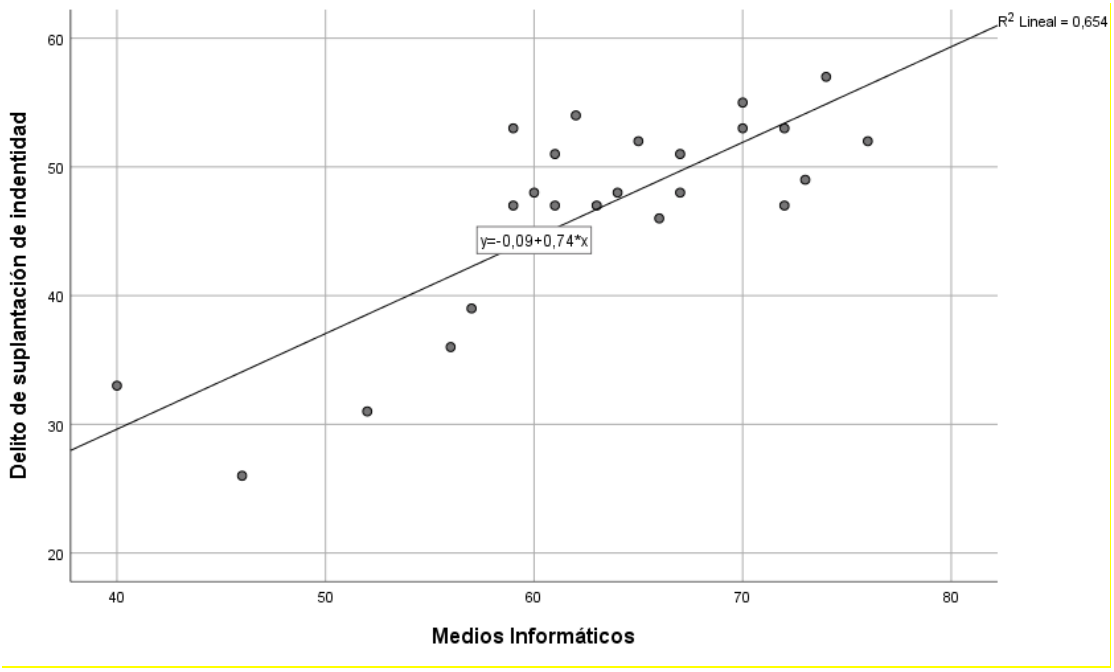
Análisis de los Coeficientes del Modelo 1

Modelo 1	Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.
	B	Desv. Error	Beta		
(Constante)	-,094	7,163		-,013	,990
Medios informáticos	,743	,113	,808	6,588	,000

Del análisis de los coeficientes del Modelo 1, se advierte que la variable Medios Informáticos presenta un nivel de significancia menor a 0.05 (sig. = 0.000), lo que indica que su influencia sobre el Delito de Suplantación de Identidad es estadísticamente significativa. Esto permite afirmar que los medios informáticos tienen un impacto considerable en la ocurrencia de este tipo de delito. En resumen, el uso o disponibilidad de medios informáticos se relaciona de manera significativa con la incidencia del delito de suplantación de identidad en el contexto analizado.

Figura 6

Gráfico de dispersión del modelo 1



El gráfico muestra la relación entre la variable independiente medios informáticos (V1) y la variable dependiente delito de suplantación de identidad (V2). Cada punto representa una observación empírica, mientras que la línea recta representa el ajuste de la regresión lineal simple entre ambas variables. Este modelo indica que por cada unidad de incremento en el uso de medios informáticos, se espera un aumento de aproximadamente 0,74 unidades en la incidencia del delito de suplantación de identidad. Aunque el valor del intercepto (-0,09) tiene

una interpretación matemática, su relevancia práctica es limitada dado que no tiene sentido analizar el delito en ausencia total de medios informáticos.

El coeficiente de determinación mostrado en el gráfico es $R^2 = 0,654$, lo que confirma que el 65,4 % de la variabilidad en el delito de suplantación de identidad puede explicarse por la variación en los medios informáticos. Esta proporción refleja un grado considerable de ajuste del modelo, indicando que la relación es estadísticamente significativa y con una tendencia clara.

b) Hipótesis específicas

H_1: Los medios informáticos influyen significativamente en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.

H0: Los medios informáticos no influyen significativamente en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.

Tabla 17

Correlación entre la variable medios informáticos y la dimensión apropiación de datos por medios convencionales o informáticos.

		Medios informáticos	Apropiación de datos por medios convencionales o informáticos
Medios informáticos	Correlación de Pearson	1	,653**
	Sig. (bilateral)		,000
	N	25	25
Apropiación de datos por medios convencionales o informáticos	Correlación de Pearson	,653**	1
	Sig. (bilateral)	,000	
	N	25	25

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

La Tabla 17 evidencia una correlación positiva moderada con un coeficiente de Pearson r=0.653 y un nivel de significancia de p=0.00, inferior al umbral establecido en 0.05. Estos resultados permiten rechazar la hipótesis nula, y confirman que los medios informáticos influyen significativamente en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024. Estos hallazgos indican que el uso de tecnologías digitales facilita y potencia las prácticas ilícitas de apropiación de información personal.

Tabla 18

Resumen del modelo 2

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
2	,653[a]	,427	,402	1,812

La Tabla 18 presenta un coeficiente de determinación (R^2) de 0,427, lo que indica que el 42,7 % de la variabilidad observada en la apropiación de datos por medios convencionales o informáticos puede ser explicada por el uso o disponibilidad de medios informáticos. Esto permite inferir que el uso de recursos tecnológicos está vinculado, en una proporción considerable, con la ocurrencia de apropiaciones indebidas de información. En ese sentido, los medios informáticos no solo actúan como instrumentos de acceso y difusión de datos, sino que también se convierten en una vía a través de la cual se facilita este tipo de conductas.

Tabla 19

ANOVA - Modelo 2

Modelo 2	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	56,257	1	56,257	17,137	,000[b]
Residuo	75,503	23	3,283		
Total	131,760	24			

En la Tabla 19 se evidencian los resultados del análisis ANOVA, en el cual el modelo 2 presenta un nivel de significancia inferior a 0.05, lo cual demuestra que existe sustento estadístico para establecer un modelo de regresión lineal entre las variables Medios Informáticos y Apropiación de datos por medios convencionales o informáticos.

Tabla 20

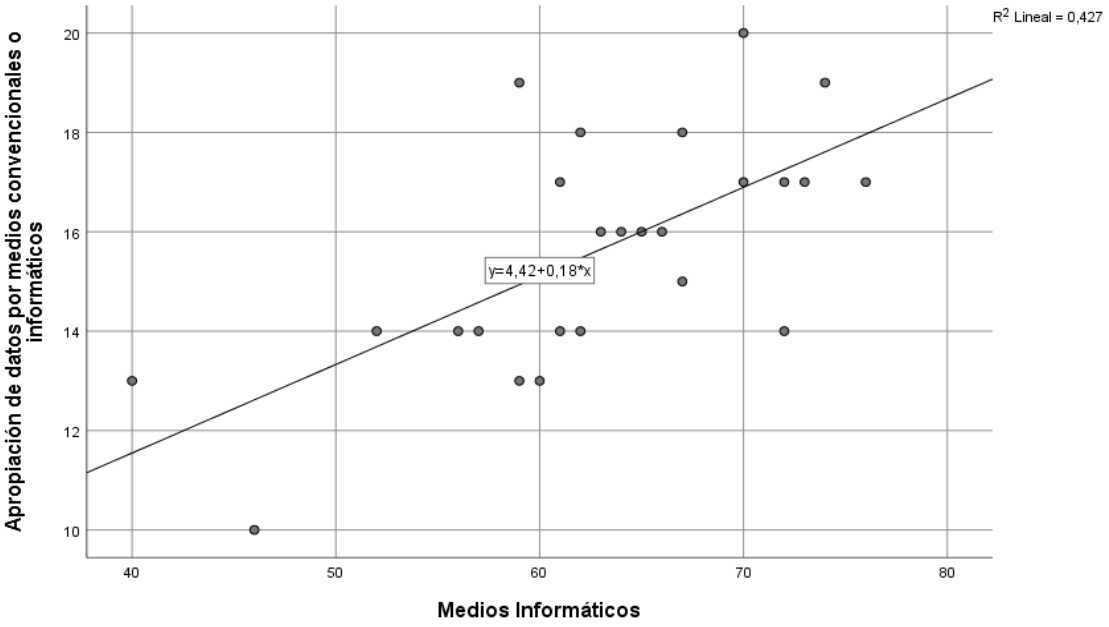
Análisis de los Coeficientes del Modelo 2

Modelo 2	Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.
	B	Desv. Error	Beta		
(Constante)	4,419	2,735		1,616	,120
Medios informáticos	,178	,043	,653	4,140	,000

Del análisis de los coeficientes del Modelo 2, se advierte que la variable Medios Informáticos presenta un nivel de significancia menor a 0.05 (sig. = 0.000), lo que indica que su influencia sobre la Apropiación de datos por medios convencionales o Informáticos es estadísticamente significativa. Esto permite afirmar que los medios informáticos tienen un impacto considerable en la ocurrencia de este tipo de delito. En resumen, el uso o disponibilidad de medios informáticos se relaciona de manera significativa con la apropiación de datos por medios convencionales o informáticos en el contexto analizado.

Figura 7

Gráfico de dispersión del modelo 2



El gráfico muestra la relación entre la variable independiente medios informáticos y la variable dependiente apropiación de datos por medios convencionales o informáticos. Cada punto representa una observación empírica, mientras que la línea recta corresponde al ajuste de una regresión lineal simple entre ambas variables. El modelo indica que, por cada unidad de incremento en el uso de medios informáticos, se espera un aumento promedio de aproximadamente 0,18 unidades en la apropiación de datos. Aunque el valor del intercepto (4,42) posee una interpretación matemática, es el valor estimado de la variable dependiente cuando el uso de medios informáticos es cero. El coeficiente de determinación ($R^2 = 0,427$) indica que el 42,7 % de la variabilidad en la apropiación de datos puede explicarse por las variaciones en el uso de medios informáticos. Este valor sugiere un grado moderado de ajuste del modelo, lo que evidencia una relación positiva y estadísticamente significativa entre las variables analizadas.

H_1: Los medios informáticos influyen significativamente en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.

H0: Los medios informáticos no influyen significativamente en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.

Tabla 21

Correlación entre la variable medios informáticos y la dimensión transferencia o cesión de datos personales.

		Medios informáticos	Transferencia o cesión de datos personales
Medios informáticos	Correlación de Pearson	1	,767**
	Sig. (bilateral)		,000
	N	25	25
Transferencia o cesión de datos personales	Correlación de Pearson	,767**	1
	Sig. (bilateral)	,000	
	N	25	25

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

La Tabla 21 evidencia una correlación positiva alta con un coeficiente de Pearson r=0.767 y un nivel de significancia de p=0.00, inferior al umbral establecido en 0.05. Estos resultados permiten rechazar la hipótesis nula, y confirman que los medios informáticos influyen significativamente en la transferencia o cesión de datos personales, Lima, periodo 2023-2024. Estos hallazgos indican que las plataformas digitales y las tecnologías de la información se han convertido en canales clave para la difusión no autorizada de datos personales, lo que expone a los individuos a mayores riesgos de vulneración de su privacidad y subraya la necesidad de reforzar los controles de seguridad y las políticas de protección de la información en entornos digitales.

Tabla 22

Resumen del modelo 3

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
3	,767[a]	,588	,570	2,091

La Tabla 22 presenta un coeficiente de determinación (R^2) de 0,558, lo que indica que el 55,8 % de la variabilidad observada en la transferencia o cesión de datos personales puede ser explicada por el uso o disponibilidad de medios informáticos. Es decir, a medida que se intensifica el uso de estos recursos tecnológicos, también tiende a incrementarse la incidencia de dicho delito. Este resultado sugiere que los medios informáticos ejercen una influencia significativa en la ocurrencia del delito analizado, por lo que deben considerarse como un elemento clave en el diseño de estrategias preventivas, normativas de control y políticas públicas orientadas a mitigar los delitos cibernéticos.

Tabla 23

ANOVA - Modelo 3

Modelo 3	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	143,229	1	143,229	32,769	,000[b]
Residuo	100,531	23	4,371		
Total	243,760	24			

La Tabla 23 muestra los resultados del análisis ANOVA, en el cual se evidencia que el modelo 3 presenta un nivel de significancia inferior a 0.05, lo cual evidencia que existe sustento estadístico para establecer un modelo de regresión lineal entre las variables “Medios Informáticos” y “Transferencia o cesión de datos personales”.

Tabla 24

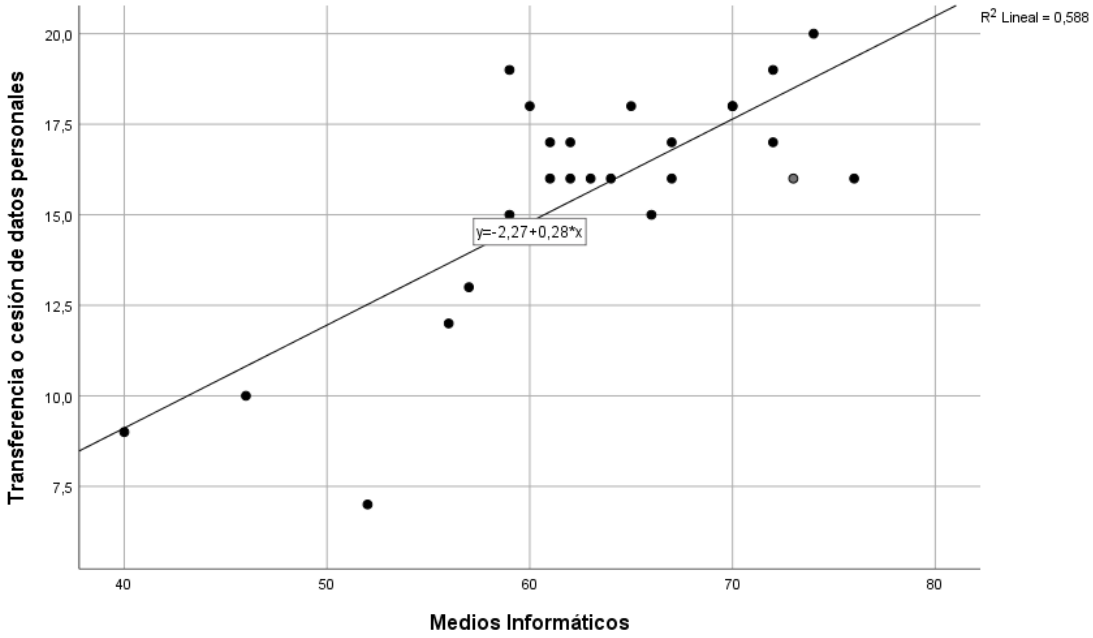
Análisis de los Coeficientes del Modelo 3

Modelo 3	Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.
	B	Desv. Error	Beta		
(Constante)	-2,265	3,156		-,718	,480
Medios informáticos	,284	,050	,767	5,724	,000

Del análisis de los coeficientes del Modelo 3, se advierte que la variable medios informáticos presenta un nivel de significancia menor a 0.05 (sig. = 0.000), lo que indica que su influencia sobre la transferencia o cesión de datos personales es estadísticamente significativa. Esto permite afirmar que los medios informáticos tienen un impacto considerable en la ocurrencia de este tipo de fenómeno. Por consiguiente, el uso o disponibilidad de medios informáticos se relaciona de manera significativa con la incidencia de transferencia o cesión de datos personales en el contexto analizado, lo que subraya la importancia de estos recursos tecnológicos en la transferencia no autorizada de datos.

Figura 8

Gráfico de dispersión del modelo 3



Este gráfico muestra una regresión lineal entre los medios informáticos, la transferencia o cesión de datos personales, lo cual refleja una relación positiva entre ambas variables. Es decir, conforme aumenta el uso de medios informáticos, también aumenta la transferencia o cesión de datos personales. Este comportamiento queda reflejado en la pendiente positiva de la recta de regresión, cuyo valor es 0,28. Por cada unidad de incremento en los medios informáticos, se espera un aumento de 0.28 unidades en la transferencia de datos personales. En cuanto al coeficiente de determinación ($R^2 = 0.588$), indica que aproximadamente el 58.8 % de la variabilidad observada en la transferencia de datos personales puede ser explicada por el uso de medios informáticos. Este valor sugiere que existe una correlación moderada entre las dos variables.

En resumen, el análisis revela que existe una correlación directa entre el uso de medios informáticos y la transferencia o cesión de datos personales. Esto sugiere que a medida que

aumenta la digitalización, también lo hace la exposición o el intercambio de datos personales, lo que podría tener implicaciones en la protección de la privacidad y la seguridad digital

H_1: Los medios informáticos influyen significativamente en la utilización de datos personales, Lima, periodo 2023-2024.

H0: Los medios informáticos no influyen significativamente en la utilización de datos personales, Lima, periodo 2023-2024.

Tabla 25

Correlación entre las variables medios informáticos y la dimensión utilización de datos personales.

		Medios informáticos	Utilización de datos personales
Medios informáticos	Correlación de Pearson	1	,721**
	Sig. (bilateral)		,000
	N	25	25
Utilización de datos personales	Correlación de Pearson	,721**	1
	Sig. (bilateral)	,000	
	N	25	25

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

La Tabla 25 evidencia una correlación positiva alta con un coeficiente de Pearson r=0.721 y un nivel de significancia de p=0.00, inferior al umbral establecido en 0.05. Estos resultados permiten rechazar la hipótesis nula, y confirman que los medios informáticos influyen significativamente en la utilización de datos personales, Lima, periodo 2023-2024. Estos hallazgos indican que el acceso y manipulación de datos personales a través de medios informáticos se ha intensificado, facilitando su uso indebido en actividades ilícitas como fraudes, suplantación de identidad y otros delitos cibernéticos.

Tabla 26

Resumen del modelo 4

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
4	,721[a]	,519	,498	2,367

La Tabla 26 muestra un coeficiente de determinación (R^2) de 0.519, lo que indica que el 51.9 % de la variabilidad observada en la utilización indebida de datos personales puede ser explicada por el uso o disponibilidad de medios informáticos. Este resultado evidencia que, a mayor uso de recursos tecnológicos, mayor es la incidencia de este tipo de delito, lo cual confirma una relación significativa entre ambas variables. En consecuencia, se concluye que los medios informáticos ejercen una influencia sustancial en la comisión del delito analizado, razón por la cual deben considerarse un elemento crítico en el diseño de estrategias preventivas, normativas de control y políticas públicas destinadas a mitigar los delitos informáticos.

Tabla 27

ANOVA - Modelo 4

Modelo 2	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	139,141	1	139,141	24,835	,000[b]
Residuo	128,859	23	5,603		
Total	268,000	24			

La Tabla 27 muestra los resultados del análisis ANOVA, en el cual se demuestra que el modelo 2 presenta un nivel de significancia inferior a 0.05, lo cual evidencia que existe sustento estadístico para establecer un modelo de regresión lineal entre las variables Medios Informáticos y Utilización de datos personales.

Tabla 28

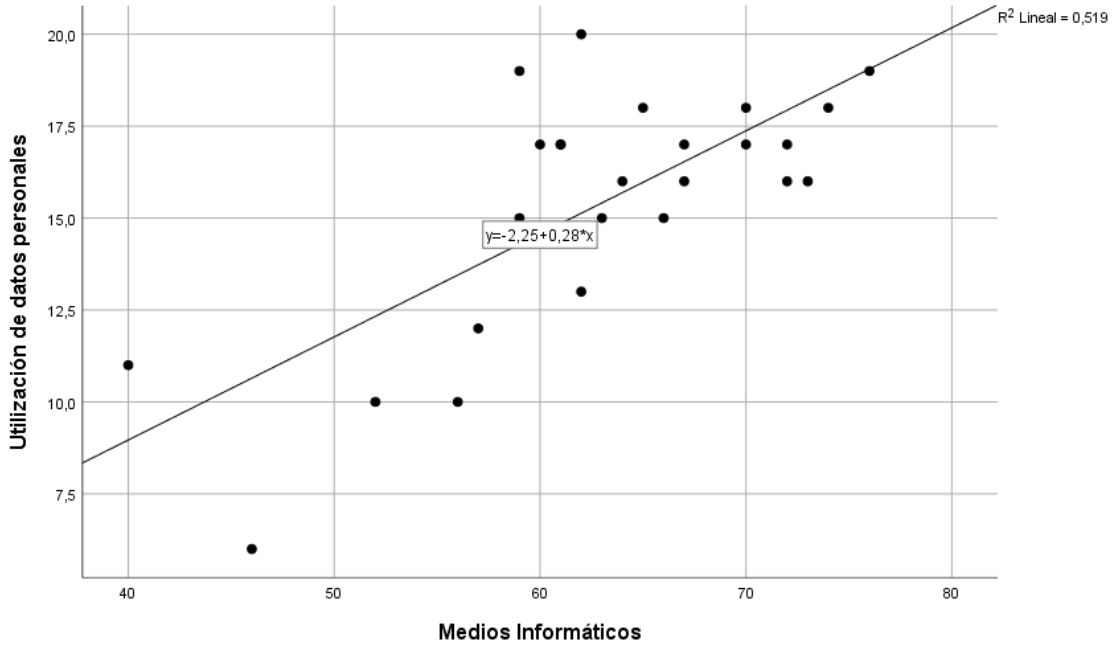
Análisis de los Coeficientes del Modelo 4

Modelo 4	Coeficientes no estandarizados		Coeficientes estandarizados	t	Sig.
	B	Desv. Error	Beta		
(Constante)	-2,248	3,573		-,629	,535
Medios informáticos	,280	,056	,721	4,983	,000

Del análisis de los coeficientes del Modelo 4, se advierte que la variable Medios Informáticos presenta un nivel de significancia menor a 0.05 (sig. = 0.000), lo cual indica que su influencia sobre la Utilización de datos personales es estadísticamente significativa. Esto permite afirmar que los medios informáticos tienen un impacto considerable en la ocurrencia de este fenómeno. En resumen, el uso o disponibilidad de medios informáticos se relaciona de manera significativa con la utilización de datos personales en el contexto analizado.

Figura 9

Gráfico de dispersión del modelo 4



El gráfico muestra la relación entre la variable independiente medios informáticos y la variable dependiente utilización de datos personales. Cada punto representa una observación empírica, mientras que la línea recta representa el ajuste de la regresión lineal simple entre ambas variables. Este modelo indica que, por cada unidad de incremento en el uso de medios informáticos, se espera un aumento de aproximadamente 0,28 unidades en la utilización de datos personales. Aunque el valor del intercepto (-2,25) tiene una interpretación matemática, su relevancia práctica es limitada dado que no tiene sentido analizar el delito en ausencia total de medios informáticos.

El coeficiente de determinación ($R^2 = 0,519$) revela que aproximadamente el 51,9 % de la variabilidad en la utilización de datos personales puede ser explicada por la variación en los medios informáticos, lo cual indica una relación estadísticamente significativa entre ambas variables y una tendencia creciente clara.

5.2. Discusión

Los resultados de la presente investigación confirman que los medios informáticos influyen significativamente en el delito de suplantación de identidad en Lima durante el periodo 2023-2024. El análisis estadístico mostró una correlación positiva alta ($r = 0.808$) y un nivel de significancia $p = 0.000$, lo que indica una fuerte relación entre el uso de tecnologías digitales y la incidencia de este tipo de delitos. A pesar de que el número de denuncias disminuyó de 3784 en 2023 a 3058 en 2024, las pérdidas económicas aumentaron de S/ 10,273,832.20 a S/ 13,473,155.68, lo que refleja un incremento en la sofisticación y el impacto financiero de estos delitos.

Estos hallazgos son consistentes con los resultados de Monja (2022), quien investigó la suplantación de identidad en entidades bancarias. Monja encontró que, aunque los bancos han adoptado tecnologías avanzadas para prevenir fraudes, estas no han sido suficientes para eliminar el problema. Esto coincide con los hallazgos del presente estudio, donde, a pesar de los esfuerzos por mejorar la seguridad, la magnitud y el impacto económico de los delitos continúan en aumento.

Por su parte, Cervantes (2021) encontró que existe relación directa entre la firma electrónica basada en reconocimiento facial y el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú. Estos hallazgos indican que la adopción de tecnologías como la firma electrónica biométrica podría reducir significativamente la suplantación de identidad. Además, complementan los hallazgos de la presente investigación, donde se resalta la necesidad de implementar tecnologías más seguras y sofisticadas para proteger la información personal, como el uso de inteligencia artificial y reconocimiento facial.

A nivel internacional, Securelist (2021) indica que en Brasil, aunque el país implementó un sistema de anti-phishing que neutralizó más de 434 millones de ataques en 2020, los delitos informáticos siguieron ocurriendo, con una incidencia del 19.94 %. Esta tendencia también se

observa en Portugal (19.73 %) y Francia (17.90 %), lo que evidencia que, aunque los países avanzan en la implementación de tecnologías de protección, la sofisticación de los delincuentes cibernéticos sigue superando las medidas de seguridad. Esto se refleja en los resultados del presente estudio, donde, a pesar de la disminución en el número de denuncias, las pérdidas económicas aumentaron significativamente, mostrando que los delitos son cada vez más complejos y costosos.

El primer objetivo específico de esta investigación fue determinar la influencia de los medios informáticos en la apropiación de datos por medios convencionales o informáticos. Los resultados obtenidos muestran una correlación positiva moderada con un coeficiente de Pearson $r = 0.653$ y un nivel de significancia de $p = 0.00$, inferior al umbral de 0.05. Esto indica que existe una relación significativa entre el uso de tecnologías informáticas y la apropiación indebida de datos, destacando la necesidad de implementar estrategias de ciberseguridad más robustas.

Estos hallazgos coinciden con los resultados de Lara et al. (2024), quienes enfatizan la importancia de combatir la suplantación de identidad en la sociedad actual. Su estudio revela que este delito puede manifestarse de diversas formas en las redes sociales, exponiendo a los usuarios a riesgos significativos para su información personal y su reputación. Al igual que en la presente investigación, concluyen que la protección de los datos personales debe ser una prioridad no solo individual, sino institucional y gubernamental, lo cual refuerza la necesidad de políticas públicas y campañas de concientización que disminuyan la vulnerabilidad frente a estos delitos.

Por otro lado, Moreno et al. (2022) abordaron el delito de suplantación digital desde una perspectiva legal, enfocándose en la necesidad de una regulación jurídica adecuada para garantizar el derecho a la identidad. Sus resultados revelaron que en muchos Estados existe una regulación insuficiente o inexistente respecto a la suplantación digital, lo que agrava la situación ante el creciente uso de tecnologías en la vida cotidiana. Esto se alinea con los

hallazgos del presente estudio, que reflejan cómo la falta de normativas claras y actualizadas puede facilitar la apropiación indebida de datos. Moreno et al. proponen la creación de una normativa global mediante tratados internacionales, lo cual complementa la necesidad detectada en nuestra investigación de fortalecer los marcos legales locales para enfrentar estos delitos de manera efectiva.

Finalmente, el estudio de Sandoval (2020), centrado en la suplantación de identidad en la red social Facebook, aporta una perspectiva legal relevante al debate. Su investigación determinó que el 94 % de los operadores de justicia encuestados consideran esencial que este delito sea sancionado adecuadamente. Esta conclusión resalta la ineficiencia del artículo 132 en su forma actual para imponer sanciones justas, mostrando la necesidad de una reforma legislativa. Estos resultados complementan el presente estudio, que muestra cómo la apropiación de datos a través de medios informáticos sigue siendo un problema significativo, en parte debido a la falta de sanciones claras y efectivas.

Con respecto al segundo objetivo específico, en la cual se buscó determinar la influencia de los medios informáticos en la transferencia o cesión de datos personales en Lima durante el periodo 2023-2024, los resultados obtenidos muestran una correlación positiva alta con un coeficiente de Pearson=0.767 y un nivel de significancia de p=0.00. Esto confirma que los medios informáticos influyen de manera significativa en la difusión no autorizada de datos personales. La alta correlación encontrada indica que las plataformas digitales y las tecnologías de la información se convirtieron en canales fundamentales para la vulneración de la privacidad, destacando la necesidad de reforzar los controles de seguridad u las políticas de protección de datos.

Estos hallazgos coinciden con los resultados de Basurto et al. (2022), quienes realizaron un análisis jurídico sobre la responsabilidad bancaria frente a delitos informáticos, donde se evidencia que si bien el uso de internet ha agilizado diversas actividades tanto económicas

como sociales, también ha incrementado la exposición de los usuarios a conductas delictivas, incluyendo el fraude digital y la apropiación indebida de datos personales. Además subrayan que el avance de la tecnología ha facilitado el almacenamiento masivo de información en dispositivos digitales, lo que amplía las oportunidades para la transferencia no autorizada de datos, evidenciando la necesidad de que las instituciones financieras y otras entidades refuercen sus protocolos de seguridad para proteger la información sensible de sus clientes.

Por su parte, Vélez (2022) llevó a cabo un estudio centrado en el hurto por medios informáticos en Colombia, evidenciando las limitaciones del desarrollo normativo en la región para combatir este tipo de delitos. En sus hallazgos muestra que, aunque la legislación colombiana ha comenzado a reconocer la importancia de aspectos tecnológicos en el ámbito legal, la respuesta institucional ha sido tardía. Por ejemplo, recién en el 2011 se creó una policía especializada en ciberdelitos, lo cual dejó en desventaja a las autoridades frente a los delincuentes cibernéticos que dominan estas tecnologías. Este hallazgo resalta la importancia de fortalecer las capacidades institucionales para enfrentar de manera efectiva la cesión no autorizada de datos personales, lo cual también es importante dentro del contexto peruano. La correlación alta encontrada en nuestro estudio sugiere que, además de reforzar las medidas de seguridad tecnológica, es necesario actualizar y ampliar la legislación nacional para estar a la par con la evolución de los delitos informáticos.

En síntesis, tanto los resultados de Basurto et al. (2022) como los de Vélez (2022) refuerzan la conclusión de que la transferencia no autorizada de datos personales es un problema creciente, facilitado por el desarrollo de las tecnologías informáticas y la insuficiencia de normativas actualizadas. La evidencia indica que la solución a esta problemática debe ser integral, combinando mejoras en ciberseguridad, actualización legislativa y fortalecimiento institucional para proteger adecuadamente la privacidad de los individuos en entornos digitales.

Finalmente, el tercer objetivo específico de esta investigación fue determinar la influencia de los medios informáticos en la utilización de datos personales en Lima durante el periodo 2023-2024. Los resultados obtenidos revelan una correlación positiva alta con un coeficiente de Pearson $r = 0.721$ y un nivel de significancia de $p = 0.00$, valor inferior al umbral de 0.05. Estos hallazgos confirman que los medios informáticos influyen de manera significativa en la utilización indebida de datos personales, evidenciando cómo las tecnologías de la información han facilitado la explotación de información personal, lo que representa un riesgo creciente para la seguridad y privacidad de los ciudadanos.

Este resultado se alinea con el estudio de Aldecoa (2020), quien investigó cómo los medios informáticos favorecen la comisión del delito de suplantación de identidad. Aldecoa concluye que la falta de filtros adecuados y mecanismos efectivos de prevención ha permitido el aumento de estos delitos. La investigación destaca que la regulación y fiscalización actuales son insuficientes, y se requiere de una mayor vigilancia estatal para frenar el uso indebido de datos personales. Estos hallazgos complementan la presente investigación, ya que la alta correlación identificada demuestra la necesidad urgente de establecer políticas más estrictas que regulen el acceso y uso de información personal en entornos digitales.

De manera similar, Monja (2022) abordó los delitos informáticos, con un enfoque en la suplantación de identidad en las entidades bancarias. Sus hallazgos señalan que, aunque los bancos han adoptado tecnologías inteligentes para prevenir fraudes, estas medidas aún resultan insuficientes para detener la utilización indebida de datos personales. Monja concluye que es necesario implementar nuevos métodos de detección y fortalecer las sanciones legales para los delincuentes, dada la gravedad del impacto de estos delitos. Esta perspectiva refuerza la necesidad de no solo mejorar la infraestructura tecnológica, sino también de incrementar la concientización y formación de los usuarios en prácticas seguras para la protección de sus datos.

En conjunto, los resultados del presente estudio y los hallazgos de Aldecoa (2020) y Monja (2022) subrayan que el crecimiento de la utilización indebida de datos personales está directamente relacionado con el desarrollo de los medios informáticos y la falta de medidas preventivas adecuadas. Por lo tanto, es fundamental que tanto el sector público como el privado adopten estrategias integrales que combinen el fortalecimiento de la ciberseguridad, la actualización normativa y la promoción de buenas prácticas digitales entre los ciudadanos. Esta acción conjunta permitirá mitigar los riesgos asociados al uso indebido de datos personales y garantizar una mayor protección de la privacidad en el entorno digital

CONCLUSIONES

Primera conclusión: Se determinó que los medios informáticos influyen significativamente en el delito de suplantación de identidad en Lima durante el periodo 2023-2024, como lo indica el análisis estadístico, que reveló un nivel de significancia de $p = 0.000$ y un coeficiente de Pearson de $r = 0.808$, lo que señala una alta correlación positiva entre las variables estudiadas. A pesar de que el número de denuncias por suplantación de identidad disminuyó de 3,784 casos en 2023 a 3,058 en 2024, las pérdidas económicas aumentaron del 2023, con S/ 10,273,832.20 y en el 2024 con S/ 13,473,155.68, lo que representa un incremento de S/ 3,199,323.48. Para evidenciar esta relación causal, se identificaron indicadores claves como la reproducción de datos, la experticia en el manejo de datos ilícitos y la comercialización de grandes bases de datos. Asimismo, para reforzar esta conclusión, Monja (2022) señala que, a pesar de los esfuerzos de los bancos peruanos por implementar tecnologías de seguridad, estas no han sido suficientes para frenar el avance del delito, lo cual coincide con el incremento del impacto económico observado en el presente estudio y reflejando la necesidad de fortalecer las medidas de ciberseguridad y prevención.

Segunda conclusión: Se determinó que los medios informáticos influyen significativamente en la apropiación de datos por medios convencionales o digitales en Lima en el 2023-2024. Los resultados estadísticos mostraron un nivel de significancia de $p = 0.000$, inferior al umbral de 0.05 y un coeficiente de Pearson de $r = 0.653$, lo que evidencia una correlación positiva moderada. Para evidenciar esta relación causal entre los medios informáticos y la apropiación de datos por medios convencionales o informáticos, se identificó indicadores clave, como la reproducción de datos, experiencia o pericia, apropiación de soportes lógicos y la usurpación de bienes incorporados. Asimismo, para fundamentar esta síntesis, Sandoval (2020) señala que las tecnologías digitales han facilitado la apropiación

ilícita de información personal, incrementando la vulnerabilidad de los usuarios frente a delitos cibernéticos y resaltando la necesidad de implementar medidas más rigurosas de seguridad informática, como la reformulación del artículo 132 del Código Penal.

Tercera conclusión: Se determinó que los medios informáticos influyen significativamente en la transferencia o cesión de datos personales en Lima durante el periodo 2023-2024. Los resultados inferenciales mostraron un nivel de significancia de $p = 0.000$ y un coeficiente de Pearson de $r = 0.767$, lo que evidencia una correlación positiva alta. Para evidenciar esta relación causal entre los medios informáticos y la transferencia o cesión de datos personales se identificaron indicadores claves, como la reproducción de datos, datos obtenidos de manera ilícita, comercialización previa de grandes bases de datos de personas, experticia o pericia y archivos. Asimismo, para reforzar esta síntesis, Cervantes (2021) señala que la adopción de la firma electrónica facial podría reducir significativamente los casos de suplantación de identidad, sugiriendo que la transición hacia métodos de verificación digital más seguros es importante para proteger la información personal. Por lo tanto, este hallazgo confirma que el uso de tecnologías digitales facilita y amplifica la transferencia no autorizada de información personal, incrementando los riesgos asociados al manejo inadecuado de datos y destacando la necesidad de reforzar las políticas de protección y confidencialidad en entornos informáticos.

Cuarta conclusión: Se determinó que los medios informáticos influyen significativamente en la utilización de datos personales en Lima durante el periodo 2023-2024. Los resultados inferenciales de la hipótesis específica mostraron un nivel de significancia de $p = 0.000$, inferior al umbral de 0.05, y un coeficiente de Pearson de $r = 0.721$**,** lo que evidencia una correlación positiva alta entre las variables analizadas. Para sustentar esta relación causal entre los medios informáticos y la utilización de datos personales, se identificó indicadores

clave como la reproducción de datos, la experticia o pericia, los archivos digitales y la producción de actos o consecuencias legales derivados del uso indebido de dicha información. Estos indicadores permiten demostrar cómo los medios tecnológicos facilitan el acceso, manipulación y uso no autorizado de datos personales. Asimismo, para reforzar esta conclusión, Aldecoa (2020) sostiene que los medios informáticos favorecen la comisión del delito de suplantación de identidad, y que la regulación y fiscalización actuales resultan insuficientes. El autor destaca la necesidad de una mayor vigilancia estatal y de políticas más estrictas que regulen el acceso y uso de la información personal en entornos digitales, lo cual coincide con los hallazgos del presente estudio.

RECOMENDACIONES

Primera recomendación: Se recomienda modificar la Ley N° 30096 sobre delitos informáticos, dado que la actual regulación en el país presenta deficiencias en comparación con legislaciones internacionales más estrictas. La actualización de esta normativa debe incluir medidas coercitivas más severas para disuadir y sancionar de manera efectiva a quienes cometen delitos informáticos, alineándose con los estándares de países que han logrado reducir significativamente estos ilícitos.

Segunda recomendación: Es necesario reformar el artículo 9 de la Ley N° 30096, con el objetivo de fortalecer el control y la fiscalización de los delitos de suplantación de identidad. Esta modificación debe contemplar sanciones más severas y específicas para los infractores, contribuyendo así a la reducción de casos de suplantación de identidad en el país.

Tercera recomendación: Se insta a las autoridades competentes a desarrollar un nuevo marco legal integral que brinde una protección más robusta a los usuarios frente al delito de suplantación de identidad. Este marco debe ir más allá de los controles temporales, anticipándose a futuras amenazas tecnológicas y garantizando la adaptación de la normativa frente a las innovaciones en los medios informáticos.

Cuarta recomendación: Se sugiere la implementación de tecnologías de inteligencia artificial, especialmente aquellas basadas en reconocimiento facial, para prevenir la utilización no autorizada de datos personales. Esta medida, que ya ha demostrado ser eficaz en varios países, puede mejorar significativamente la seguridad digital, disminuyendo la incidencia de delitos relacionados con la suplantación de identidad.

REFERENCIAS

Ahmad, T. (2020). Corona virus: Pandemic and Wolk from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN*. https://doi.org/10.2139/ssrn.3568830

Aldecoa, M. (2020). El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019. *[Tesis de pregrado, Universidad César Vallejo].* respositorio institucional, Lima. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/61838/Aldecoa_JMR-SD.pdf?sequence=1&isAllowed=y

Aparicio, O. (2018). Uso y apropiación de las TIC en educación. *Revista interamericana de investigación, educación y, 12*(1), 211-227. https://doi.org/10.15332/s1657-107X.2019.0001.04

Arancibia, T. (2021). Peritaje informático en redes sociales. *Revista PGI*(7), 100-103. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/120

Aranda, F. (2021). *Derecho y las nuevas tecnologías: La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español.* Dykinson.

Arias, J. L. (2021). *Técnicas e instrumentos: Investigación científica* (1 ed.). Arequipa, Péru: Enfoques consulting. https://gc.scalahed.com/recursos/files/r161r/w26118w/Tecnicas%20e%20instrumentos.pdf

Avendaño, J., & Avendaño, F. (2017). *Derechos reales.* PUCP. https://books.google.es/books?hl=es&lr=&id=naDNDwAAQBAJ&oi=fnd&pg=PT5&

dq=Derechos+reales&ots=2BZrbiDZod&sig=S_pSk8shRi5nazmNFisNulyPIic#v=onepage&q=Derechos%20reales&f=false

Benavente Chorres, H. (2021). *La pragmática de la imputación penal.* Bosch Procesal.

Broadhurst, R. (2021). Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3009574

Cabrera, S., Dávalos, A., Sánchez, M., & Okamoto, J. (2019). Efectos legales y fiscales de la suplantación de identidiad digital. *Global conference on business and finance proceending, 14*(2), 242-251. https://www.researchgate.net/profile/Gerardo-Pedraza-Vega/publication/334683140_DIAGNOSTICO_DE_LOS_PROCESOS_QUE_ADELANTA_EL_CENTRO_REGIONAL_IBAGUE_EN_EL_CUMPLIMIENTO_DEL_SISTEMA_DE_INVESTIGACION/links/5d39e0d24585153e5921d5ce/DIAGNOSTICO-DE-LOS-PROCESOS-Q

Cervantes, R. (2021). La firma electrónica basado en reconocimiento facial y el riesgo de suplantación de identidad en el Colegio de Ingenieros del Perú, Consejo Departamental de Lima. *[Tesis de pregrado, Universidad Cientifica del Sur].* Roposito insitucional Universidad Científica del Sur, Lima. https://repositorio.cientifica.edu.pe/bitstream/handle/20.500.12805/1892/TL-Cervantes%20R.pdf?sequence=8&isAllowed=y

Concepción, D. N., González, E., García, R., & Miño, J. E. (2019). Metodología de la investigación: Origen y construcción de una tesis doctoral. *Revista Científica de la UCSA, 6*(1). https://doi.org/10.18004/ucsa/2409-8752/2019.006(01)076-087

Congreso de la República. (2013). *Ley Nº 30096.* https://www.leyes.congreso.gob.pe/documentos/leyes/30096.pdf

Defensoría del Pueblo. (2023). *LA CIBERDELINCUENCIA EN EL PERÚ: ESTRATEGIAS Y RETOS DEL ESTADO.* https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Dellepiane, A. (2021). *Nueva teoría de la prueba.* Temis. https://books.google.com.pe/books?id=WeBYEAAAQBAJ&printsec=frontcover

Díaz, I., Bodero, M., Ulloa, L., & Mora, D. (2022). Análisis jurídico de la responsabilidad bancaria frente a delitos informáticos. *Revista Arbitrada de Ciencias Jurídicas y Criminalísticas, 7*(2), 1144. https://dialnet.unirioja.es/servlet/articulo?codigo=8954914

Dolores, C., Capafons, J. I., Pérez, S. M., Lastenia, G., Capafons, J. I., & Prieto, P. (2019). El uso de las Nuevas Tecnologías (internet, redes sociales y videojuegos) en jovenes: un estudio con población canaria. *Revista española drogodepend, 44*(2), 26-42. https://pesquisa.bvsalud.org/portal/resource/pt/ibc-184428

Estévez, J. F. (2019). *Derecho digital* (Vol. 1052). Arazandi. https://www.aranzadilaley.es/MK/PDF/Derecho-digital/publication.pdf

Fernández, D., & Sanz, E. (2021). *Tratado de delincuencia Cibernética.* Aranzadi. https://books.google.com.pe/books?id=bipdEAAAQBAJ&printsec=frontcover

Gallardo, E. (2017). Metodología de la investigación: manual autoformativo interactivo. *Universidad Continental*. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

García, N. (2020). *Ciudadanos reemplazados por algoritmos.* Calas. https://doi.org/10.14361/9783839448915

Gobierno del Perú. (2023). *Decreto Legislativo N°1591.* https://www.gob.pe/institucion/mpfn/informes-publicaciones/5258286-decreto-legislativo-n-1591

Gobierno del Perú. (2024). *Ley N°30096.* Gob.pe. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

González, I. M. (2021). *El gobierno de la función legal en las organizaciones: Operaciones legales.* Arazandi.

Harán, J. (2021). *Malware: la principal preocupación de las empresas de América Latina*. Welivesecurity: https://www.welivesecurity.com/la-es/2021/06/08/malwareprincipal-preocupacion-empresas-america-latina/?utm_source=

Hernández, R., Fernández, C., & Baptista, M. d. (2014). *Metodología de la Investigación* (Vol. 6). México: McGRAW-HILL Education. https://doi.org/10.2307/j.ctvr43hvc.8

Huaroc, P. (2021). Delitos Informáticos. *Revista Peruana de Derecho y Economía (RPDE)*, 73-78. https://rpde.tytl.com.pe/wp-content/uploads/2021/11/09-DELITOS-INFORMATICOS.pdf

Ibáñez P., A. (2020). En materia de prueba: sobre algunos cuestionables tópicos jurisprudenciales. *Revista internacional sobre razonamiento probatorio, 1*, 75-102. https://doi.org/10.33115/udg_bib/qf.i0.2236.4

Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales. (2023). *Aconseja INAI configurar privacidad en redes sociales, para*

evitar usurpación de identidad con inteligencia artificial. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-373-23.pdf

Kaspersky. (2023). *América Latina registra 2,274 intentos de infección de malware por minuto, siendo la piratería el mayor villano*. Kaspersky: https://latam.kaspersky.com/about/press-releases/america-latina-registra-2274-intentos-de-infeccion-de-malware-por-minuto-siendo-la-pirateria-el-mayor-villano?srsltid=AfmBOopUNzA66w1YW7-67oWZqGZFQjawgtuwKyHiOMNaoF_eko4ypc-g&utm_source=

Kulikova, T., Щербакова, Т., & Сидорина, Т. (2021, 02 15). *El spam y el phishing en 2020*. SECURELIST BY KASPERSKY: https://securelist.lat/spam-and-phishing-in-2020/92784/?utm_source=facebook&utm_medium=social&utm_campaign=mx_blogs_hd0137&utm_content=sm-post&utm_term=mx_facebook_organic_pdw8eq9kev137qi

Lujardo Escobar, Y. (2016). Análisis Documental: ¿Normas establecidas? Infomed: Red de Salud de Cuba. https://files.sld.cu/bmn/files/2016/10/An%C3%A1lisis-Documental.-Normas-establecidas-el-de-la-ksa.pdf

Macías, R., Bedoya, J., Manchay, J., Nazareno, G., & Mina, R. (2024). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales. *Revista Científica Multidisciplinar G-Nerando, 5*(1), 544-561. https://doi.org/10.60100/rcmg.v5i1.212

Marcelino, M., Martínez, M., & Camacho, A. (2024). Análisis documental, un proceso de apropiación del conocimiento. *Revista Digital Universitaria, 25*(6). https://doi.org/10.22201/ceide.16076079e.2024.25.6.1

Marcos Ayjón, M. (2020). *La protección de datos de carácter personal en la justicia penal.* J. M. Bosch.

Martínez, J. (2022). Hurto a través de medios informáticos y otras conductas delictivas semejantes en Colombia en 2022. *[Tesis de pregrado, Universidad Catolica de Colombia].* repositorio institucional, Bogotá. https://repository.ucatolica.edu.co/entities/publication/341fc28a-d342-448b-a10c-a6313e159134

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología, 9*(1). https://doi.org/10.5354/0719-2584.2020.53447

Medina, M., Rojas, R., Bustamante, W., Loaiza, R., & Martel, C. C. (2023). *Metodología de la investigación: Técnicas e instrumentos de investigación* (1 ed.). Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C. http://coralito.umar.mx:8383/jspui/bitstream/123456789/1539/1/80-M%c3%a9todolog%c3%ada%2bde%2bla%2binvestigaci%c3%b3n.pdf

Mejía Lobo, M., Hurtado Gil, S., & Grisales Aguirre, A. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones. *Revista de ciencias sociales, 29*(2), 356-372. https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

Menchú, N. (2017). Creación de 3 Fichas de Observación Para el Acompañamiento Pedagógico Dirigido a 10 Directores del Sector 08-03-10 del Municipio de San

Francisco El Alto, del departamento de Totonicapán. *[Tesis de pregrado, Universidad de San Carlos de Guatemala].* repositorio institucional, Guatemala. http://biblioteca.usac.edu.gt/tesis/29/29_0413.pdf

Ministerio Público. (2021). Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada OFAEC. https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Monja, G. (2022). Delitos informáticos en las entidades bancarias -suplantación de identidad. *[Tesis de pregrado, Universidad de Las Américas].* Ropositorio institucional de Universidad de Las Américas, Lima. http://repositorio.ulasamericas.edu.pe/handle/upa/1953

Moreno, P., Paucar, C., & Cajas, C. (2022). Regulación global para evitar la suplantación de identidad digital. *Universidad Y Sociedad, 14*(6), 690-696. https://rus.ucf.edu.cu/index.php/rus/article/view/3419?utm_source=chatgpt.com

MPFN. (2024). *Suplantación de identidad.* Ministerio Público Fiscalía de la Nación. https://www.gob.pe/25712-suplantacion-de-identidad

Niño, V. (2021). *Metodología de la investigación: Diseño, ejecución e informe* (Vol. 2 da edición). Ediciones de la U. https://books.google.com.pe/books?id=WCwaEAAAQBAJ&dq=investigaci%C3%B3n+descriptiva+metodologia&hl=es&source=gbs_navlinks_s

Ojeda, Z., & Cutié, D. (2022). El derecho a la protección de datos personales en Cuba, desafíos en la era digital. *Revista IUS, 15*(48). https://doi.org/10.35487/rius.v15i48.2021.689

Organización de los Estados Americanos. (2022). *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions.* https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=667&lang=1

Pasión por el derecho. (2024). *Ley de Delitos Informáticos (Ley 30096) [actualizada].* Lp. https://lpderecho.pe/ley-delitos-informaticos-ley-30096/

Piva, G., Ruiz, W., & Lattuf, W. (2021). *La investigación del delito en el Derecho Penal Español.* Barcelona: J B Bosch Editor. https://books.google.es/books?hl=es&lr=&id=83o6EAAAQBAJ&oi=fnd&pg=PA29&dq=La+investigaci%C3%B3n+del+delito+en+el+Derecho+Penal+Espa%C3%B1ol+Bosch+Editor&ots=iSyszaQnv6&sig=d4K2zM1IH7nURUtj0RI91hD_EGc#v=onepage&q=La%20investigaci%C3%B3n%20del%20delito%20en

Ponce, M. (2024). Desafíos y respuestas legales ante los delitos informáticos en Ecuador. *Revista San Gregorio, 1*(58). https://doi.org/10.36097/rsan.v1i58.2667

Registro Nacional de la Identificación y Estado Civil. (2024). *Reniec bloqueó cerca de mil intentos de suplantaciones de identidad desde el 2020.* https://identidad.reniec.gob.pe/b/reniec-bloqueo-cerca-de-mil-intentos-de-suplantaciones-de-identidad-desde-el-2020?utm_source=chatgpt.com

Reyes, H. (2018). Problemas éticos en las publicaciones científicas. *Revista médica de Chile, 146*(3). https://doi.org/10.4067/s0034-98872018000300373

Rivera Barrantes, V. (2019). Realidad sobre la privacidad de los datos personales en Costa Rica. *E-Ciencias de la Información, 9*(2). https://doi.org/10.15517/eci.v9i2.37503

Rodríguez, J. (2018). *Circuito cerrado de televisión y seguridad electrónica* (Vol. 2). Madrid: Paraninfo.

Romero García, C. (2021). *Transmision de información por medios convencionales e informáticos* (2 ed.). IC Editorial. https://books.google.es/books?hl=es&lr=&id=Ko40EAAAQBAJ&oi=fnd&pg=PT31&dq=Transmision+de+informaci%C3%B3n+por+medios+convencionales+e+inform%C3%A1ticos&ots=XXpXNcBK7O&sig=Y3CJ51kXqrQNsJnKQkWdhA2Ri6w

Sandoval, E. (2020). El delito de difamación en la modalidad de suplantación de identidad a través de la red social Facebook. *[Tesis de pregrado, Universidad César Vallejo].* respositorio institucional, Chiclayo. https://repositorioslatinoamericanos.uchile.cl/handle/2250/3233428

Tenorio, I., & López, R. (2021). *La nueva radio* (Vol. 2). Marcombo. https://books.google.com.pe/books?id=wwlPEAAAQBAJ&printsec=frontcover

Torres Flóres, D., Rincón Ramírez, A., & Medina Moreno, L. (2022). Competencias digitales de los docentes en la Universidad de los Llanos, Colombia. *Trilogía Ciencia Tecnología Sociedad, 14*(26). https://doi.org/10.22430/21457778.2246

Vásquez, F., García , D., Valencia, M., & Gabalán, J. (2020). Análisis de la apropiación tecnológica en el adulto mayor : Más allás de la edad. *Ánfora, 27*(49). https://www.redalyc.org/journal/3578/357866371010/

Ventura, J. L. (2017). ¿Población o muestra?: Una diferencia necesaria. *Revista Cubana de Salud Pública, 43*(3), 648-649. http://scielo.sld.cu/pdf/rcsp/v43n4/spu14417.pdf

Verano, P. (2025, Marzo 7). Ciberdelincuencia en Perú aumentó un 40% en 2024: más de 42 mil denuncias por delitos informáticos. https://rpp.pe/peru/actualidad/fraudes-digitales-y-suplantacion-de-identidad-alarmantes-cifras-de-la-pnp-revelan-el-impacto-de-la-ciberdelincuencia-en-peru-noticia-1620466?ref=rpp

ANEXOS

Anexo 1 Matriz de consistencia

TÌTULO: DELITO DE SUPLANTACIÓN DE IDENTIDAD Y MEDIOS INFORMÁTICOS, LIMA, PERIODO 2023-2024

AUTORA: MAYRA YESSENIA SANCHEZ ESPEJO

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
¿De qué manera el uso de los medios informáticos influye en el delito de suplantación de identidad, periodo 2023-2024?	Determinar cómo el uso de los medios informáticos influye en el delito de suplantación de identidad, periodo 2023-2024.	Los medios informáticos influyen significativamente en el delito de suplantación de identidad, periodo 2023-2024.	**Variable 1:** MEDIOS INFORMÁTICOS			
			DIMENSIONES	**INDICADORES**	**ITEM**	**NIVELES**
			Soportes electrónicos	Archivos.	1-2	BAJO 16 -37 MEDIO 38 -59 ALTO 60 - 80
				Reproducción de datos.	3-4	
				Signos, símbolos o códigos.	5-6	
			Formas de aportación de prueba	Inspección judicial.	7-8	
				Experticia o pericia.	9-10	
				Prueba indiciaria.	11-12	
			Instrumentos de filmación	Cámaras de videovigilancia.	13-14	
				Reproductores de cintas magnetofónicas.	15-16	
PROBLEMAS SECUNDARIOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICAS**	**Variable 2:** DELITO DE SUPLANTACIÓN DE IDENTIDAD			
			DIMENSIONES	**INDICADORES**	**ITEM**	**NIVELES**
Determinar cómo el uso de los medios informáticos influye en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.	Determinar cómo el uso de los medios informáticos influye en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.	Los medios informáticos influyen significativamente en la apropiación de datos por medios convencionales o informáticos, Lima, periodo 2023-2024.	Apropiación de datos por medios convencionales o informáticos	Apropiación de soportes lógicos.	1-2	BAJO 12-28 MEDIO 29-45 ALTO 46-60
				Usurpación de bienes incorpóreos.	3-4	
Determinar cómo el uso de los medios informáticos influye en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.	Determinar cómo el uso de los medios informáticos influye en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.	Los medios informáticos influyen significativamente en la transferencia o cesión de datos personales, Lima, periodo 2023-2024.	Transferencia o cesión de datos personales	Datos obtenidos de manera ilícita.	5-6	
				Comercialización previa de grandes bases de datos de personas.	7-8	

Determinar cómo el uso de los medios informáticos influye en la utilización de datos personales, Lima, periodo 2023-2024.	Determinar cómo el uso de los medios informáticos influye en la utilización de datos personales, Lima, periodo 2023-2024.	Los medios informáticos influyen significativamente en la utilización de datos personales, Lima, periodo 2023-2024.	Utilización de datos personales	Cualidades atributivas y relacionales con el ente de imputación jurídica.	9-10	
				Producción de actos o consecuencias legales.	11-12	

TIPO Y DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA DESCRIPTIVA E INFERENCIAL
Tipo de investigación: Básica **Nivel:** Correlacional **Enfoque:** Cuantitativo **Diseño:** No experimental transeccional descriptivo.	**Población:** 128 efectivos policiales de la DIRINCRI y las denuncias DIVINDAT 2023-2024 por el delito contra la fe pública, modalidad de suplantación de identidad. **Muestra:** 25 efectivos de la DIRINCRI especialistas en el área de delitos informáticos y las denuncias DIVINDAT 2023-2024 por el delito contra la fe pública, modalidad de suplantación de identidad.	**Técnica:** Encuesta - Observación **Instrumento:** Cuestionario y ficha de observación	SPSS

Anexo 2 Matriz de operacionalización

Variables	Definición	Dimensiones	Indicadores	Ítems	Escala de medición	Instrumentos
Medios informáticos	Se definen como instrumentos complejos que poseen inteligencia artificial que permiten la realización de ciertos procesos y conductas humanas. Cabe señalar que también son considerados como mediadores para alcanzar u obtener objetivos (Rivera, 2008).	Soportes electrónicos	Archivos	1-2	Tipo Likert: (1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Indiferente, (4) De acuerdo, (5) Totalmente de acuerdo.	Encuesta (Cuestionario y ficha de observación)
			Reproducción de datos	3-4		
			Signos, símbolos o códigos	5-6		
		Formas de aportación de prueba	Inspección judicial	7-8		
			Experticia o pericia	9-10		
			Prueba indiciaria	11-12		
		Instrumentos de filmación	Cámaras de videovigilancia	13-14		
			Reproductores de cintas magnetofónicas	15-16		
Suplantación de identidad en casos de robos	Se refiere a un delito muy frecuente que consiste en hacerse pasar por otra persona para obtener algún provecho. Para aquellas personas que cometen estos delitos existen penas o multas para frenar estas acciones que perjudican a la sociedad y evita que las personas puedan vivir en sociedad (Romero, s.f).	Apropiación de datos por medios convencionales o informáticos	Apropiamiento de soportes lógicos	1-2		
			Usurpación de bienes incorpóreos	3-4		
		Transferencia o cesión de datos personales	Datos obtenidos de manera ilícita.	5-6		
			Comercialización previa de grandes bases de datos de personas.	7-8		
		Utilización de datos personales	Cualidades atributivas y relacionales con el ente de imputación jurídica.	9-10		
			Producción de actos o consecuencias legales.	11-12		

Anexo 3 Instrumento de recolección de datos

CUESTIONARIO DE LA PRIMERA VARIABLE: MEDIOS INFORMÁTICOS

INSTRUCCIONES: A continuación, encontrarás afirmaciones de la planificación estratégica. Lee cada una con mucha atención; luego, marca la respuesta que mejor te describe con una X según corresponda. Recuerda, no hay respuestas buenas, ni malas. Contesta todas las preguntas con la verdad.

OPCIONES DE RESPUESTA:

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

PROCESOS ADMINISTRATIVOS	RESPUESTAS				
	1	2	3	4	5
DIMENSIÓN: SOPORTES ELECTRÓNICOS					
1. Los soportes electrónicos poseen la capacidad de archivar información.					
2. A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.					
3. Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.					
4. Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.					
5. Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.					
6. Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.					
DIMENSIÓN 2: FORMAS DE APORTACIÓN DE PRUEBA					

7. Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.					
8. La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.					
9. Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.					
10. La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.					
11. Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.					
12. Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.					
DIMENSIÓN 3: INSTRUMENTOS DE FILMACIÓN					
13. Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.					
14. Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.					
15. Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.					
16. Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.					

CUESTIONARIO DE LA SEGUNDA VARIABLE: SUPLANTACIÓN DE IDENTIDAD

INSTRUCCIONES: A continuación, encontrarás afirmaciones de la planificación estratégica. Lee cada una con mucha atención; luego, marca la respuesta que mejor te describe con una X según corresponda. Recuerda, no hay respuestas buenas, ni malas. Contesta todas las preguntas con la verdad.

OPCIONES DE RESPUESTA:

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

PROCESOS ADMINISTRATIVOS	RESPUESTAS				
	1	2	3	4	5
DIMENSIÓN 1: APROPIACIÓN DE DATOS POR MEDIOS CONVENCIONALES O INFORMÁTICOS					
1. La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.					
2. El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.					
3. La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.					
4. Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo					
DIMENSIÓN 2: TRANSFERENCIA O CESIÓN DE DATOS PERSONALES					
5. La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.					
6. Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.					
7. La comercialización previa de grandes bases de datos de personas es un negocio muy popular					

que es gestionado por personas inescrupulosas que buscan un beneficio económico.					
8. La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.					
DIMENSIÓN 3: UTILIZACIÓN DE DATOS PERSONALES					
9. El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.					
10. Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.					
11. La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.					
12. Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.					

Anexo 4 Validación del instrumento de recolección de datos

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LOS MEDIOS INFORMÁTICOS

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN: SOPORTES ELECTRÓNICOS								
1	Los soportes electrónicos poseen la capacidad de archivar información.	X		X		X		
2	A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.	X		X		X		
3	Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.	X		X		X		
4	Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.	X		X		X		
5	Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.	X		X		X		
6	Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.	X		X		X		
DIMENSIÓN 2: FORMAS DE APORTACIÓN DE PRUEBA								

7	Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.	X		X		X		
8	La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.	X		X		X		
9	Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.	X		X		X		
10	La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.	X		X		X		
11	Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.	X		X		X		
12	Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.	X		X		X		
DIMENSIÓN 3: INSTRUMENTOS DE FILMACIÓN								
13	Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.	X		X		X		
14	Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.	X		X		X		
15	Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.	X		X		X		
16	Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: **Guerrero Muñoz, Rody** **DNI: 06773041**

Especialidad del validador: Abogado

10 DE DICIEMBRE DEL 2024

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---------- ----------

Firma

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SUPLANTACIÓN DE IDENTIDAD

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: APROPIACIÓN DE DATOS POR MEDIOS CONVENCIONALES O INFORMÁTICOS								
1	La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.	X		X		X		
2	El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.	X		X		X		
3	La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.	X		X		X		
4	Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo.	X		X		X		
DIMENSIÓN 2: TRANSFERENCIA O CESIÓN DE DATOS PERSONALES								
5	La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.	X		X		X		
6	Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.	X		X		X		
7	La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.	X		X		X		

8	La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.	X		X		X		
DIMENSIÓN 3: UTILIZACIÓN DE DATOS PERSONALES								
9	El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.	X		X		X		
10	Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.	X		X		X		
11	La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.	X		X		X		
12	Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

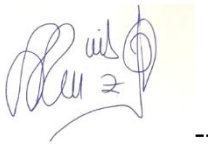
Apellidos y nombres del juez validador: **Guerrero Muñoz, Rody Anibal** **DNI: 06773041**

Especialidad del validador: Abogado

10 DE DICIEMBRE DEL 2024

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



---------- ----------

Firma

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LOS MEDIOS INFORMÁTICOS

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN: SOPORTES ELECTRÓNICOS								
1	Los soportes electrónicos poseen la capacidad de archivar información.	X		X		X		
2	A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.	X		X		X		
3	Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.	X		X		X		
4	Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.	X		X		X		
5	Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.	X		X		X		
6	Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.	X		X		X		
DIMENSIÓN 2: FORMAS DE APORTACIÓN DE PRUEBA								

7	Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.	X		X		X		
8	La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.	X		X		X		
9	Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.	X		X		X		
10	La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.	X		X		X		
11	Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.	X		X		X		
12	Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.	X		X		X		
DIMENSIÓN 3: INSTRUMENTOS DE FILMACIÓN								
13	Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.	X		X		X		
14	Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.	X		X		X		
15	Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.	X		X		X		
16	Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: **Escudero Vílchez, Fernando Emilio** **DNI: 03695876**

Especialidad del validador: Metodólogo

10 DE DICIEMBRE DEL 2024

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---------- ----------

Firma

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SUPLANTACIÓN DE IDENTIDAD

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: APROPIACIÓN DE DATOS POR MEDIOS CONVENCIONALES O INFORMÁTICOS								
1	La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.	X		X		X		
2	El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.	X		X		X		
3	La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.	X		X		X		
4	Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo.	X		X		X		
DIMENSIÓN 2: TRANSFERENCIA O CESIÓN DE DATOS PERSONALES								
5	La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.	X		X		X		
6	Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.	X		X		X		
7	La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.	X		X		X		

8	La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.	X		X		X		
DIMENSIÓN 3: UTILIZACIÓN DE DATOS PERSONALES								
9	El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.	X		X		X		
10	Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.	X		X		X		
11	La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.	X		X		X		
12	Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: **Escudero Vílchez, Fernando Emilio** **DNI: 03695876**

Especialidad del validador: Metodólogo

10 DE DICIEMBRE DEL 2024

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---------- ----------

Firma

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LOS MEDIOS INFORMÁTICOS

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN: SOPORTES ELECTRÓNICOS								
1	Los soportes electrónicos poseen la capacidad de archivar información.	X		X		X		
2	A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.	X		X		X		
3	Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.	X		X		X		
4	Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.	X		X		X		
5	Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.	X		X		X		
6	Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.	X		X		X		
DIMENSIÓN 2: FORMAS DE APORTACIÓN DE PRUEBA								

7	Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.	X		X		X		
8	La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.	X		X		X		
9	Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.	X		X		X		
10	La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.	X		X		X		
11	Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.	X		X		X		
12	Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.	X		X		X		
DIMENSIÓN 3: INSTRUMENTOS DE FILMACIÓN								
13	Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.	X		X		X		
14	Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.	X		X		X		
15	Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.	X		X		X		
16	Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: **Salazar Llerena, Silvia Liliana** **DNI: 10139161**

Especialidad del validador: Metodóloga

10 DE DICIEMBRE DEL 2024

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---------- ----------

Firma

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SUPLANTACIÓN DE IDENTIDAD

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: APROPIACIÓN DE DATOS POR MEDIOS CONVENCIONALES O INFORMÁTICOS								
1	La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.	X		X		X		
2	El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.	X		X		X		
3	La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.	X		X		X		
4	Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo.	X		X		X		
DIMENSIÓN 2: TRANSFERENCIA O CESIÓN DE DATOS PERSONALES								
5	La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.	X		X		X		
6	Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.	X		X		X		
7	La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.	X		X		X		

8	La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.	X		X		X		
DIMENSIÓN 3: UTILIZACIÓN DE DATOS PERSONALES								
9	El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.	X		X		X		
10	Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.	X		X		X		
11	La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.	X		X		X		
12	Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.	X		X		X		

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: **Salazar Llerena, Silvia Liliana** **DNI: 10139161**

Especialidad del validador: Metodóloga

10 DE DICIEMBRE DEL 2024

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---------- ----------

Firma

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LOS MEDIOS INFORMÁTICOS

DIMENSIONES / ÍTEMS		Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN: SOPORTES ELECTRÓNICOS								
1	Los soportes electrónicos poseen la capacidad de archivar información.	X		X		X		
2	A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.	X		X		X		
3	Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.	X		X		X		
4	Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.	X		X		X		
5	Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.	X		X		X		
6	Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.	X		X		X		
DIMENSIÓN 2: FORMAS DE APORTACIÓN DE PRUEBA								
7	Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.	X		X		X		

8	La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.	X		X		X		
9	Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.	X		X		X		
10	La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.	X		X		X		
11	Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.	X		X		X		
12	Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.	X		X		X		
DIMENSIÓN 3: INSTRUMENTOS DE FILMACIÓN								
13	Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.	X		X		X		
14	Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.	X		X		X		
15	Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.	X		X		X		
16	Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.	X		X		X		

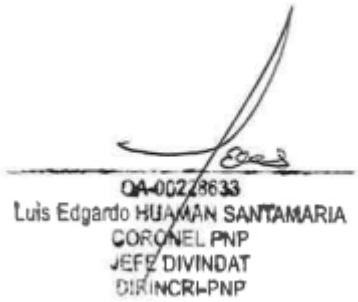
Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador:
Huaman Santamaria Luis Edgardo **DNI: 22517797**

Especialidad del validador: Coronel PNP

15 DE DICIEMBRE DEL 2024



Firma

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE SUPLANTACIÓN DE IDENTIDAD

	DIMENSIONES / ÍTEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
		Si	No	Si	No	Si	No	
DIMENSIÓN 1: APROPIACIÓN DE DATOS POR MEDIOS CONVENCIONALES O INFORMÁTICOS								
1	La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.	X		X		X		
2	El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.	X		X		X		
3	La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.	X		X		X		
4	Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo.	X		X		X		
DIMENSIÓN 2: TRANSFERENCIA O CESIÓN DE DATOS PERSONALES								
5	La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.	X		X		X		
6	Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.	X		X		X		
7	La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.	X		X		X		

8	La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.	X		X		X		
DIMENSIÓN 3: UTILIZACIÓN DE DATOS PERSONALES								
9	El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.	X		X		X		
10	Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.	X		X		X		
11	La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.	X		X		X		
12	Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.	X		X		X		

Observaciones (precisar si hay suficiencia):

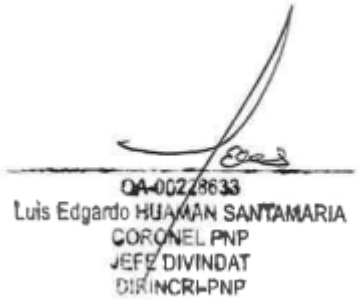
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador:
Huaman Santamaria Luis Edgardo **DNI: 22517797**

Especialidad del validador: Coronel PNP

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Firma

Anexo 5 Distribución de frecuencias

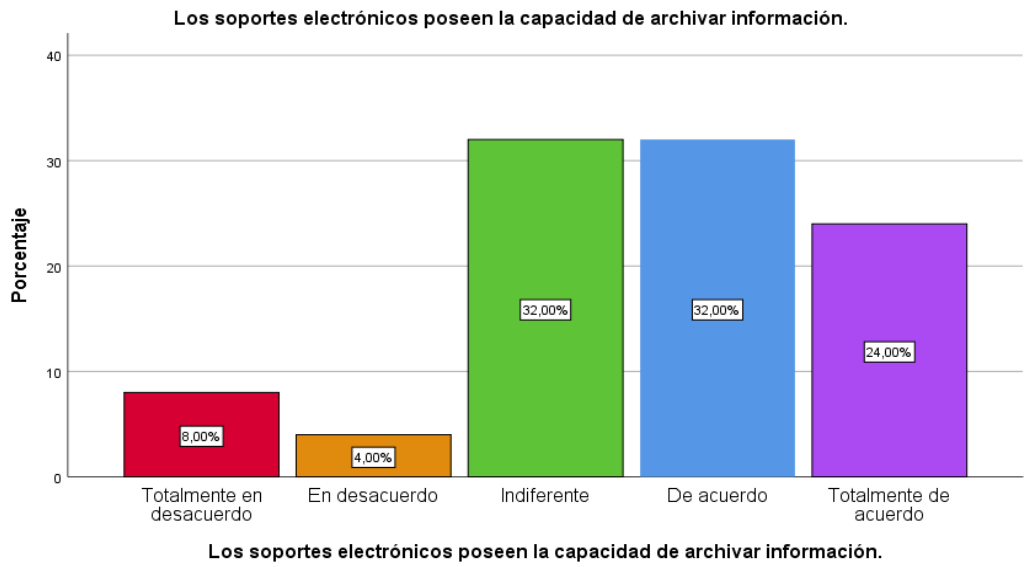
Tabla 29

Los soportes electrónicos poseen la capacidad de archivar información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	1	4,0	4,0	12,0
	Indiferente	8	32,0	32,0	44,0
	De acuerdo	8	32,0	32,0	76,0
	Totalmente de acuerdo	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Figura 10

Los soportes electrónicos poseen la capacidad de archivar información.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 32.0% tanto indiferentes como de acuerdo en considerar que los soportes electrónicos poseen la capacidad de archivar información.

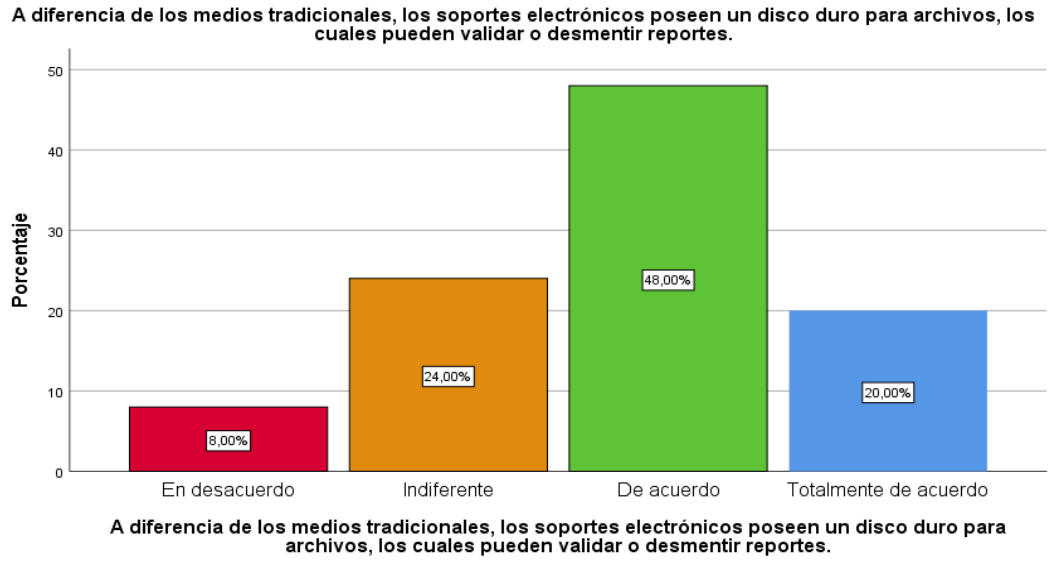
Tabla 30

A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	2	8,0	8,0	8,0
	Indiferente	6	24,0	24,0	32,0
	De acuerdo	12	48,0	48,0	80,0
	Totalmente de acuerdo	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Figura 11

A diferencia de los medios tradicionales, los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 48.00% de acuerdo en considerar que a diferencia de los medios tradicionales los soportes electrónicos poseen un disco duro para archivos, los cuales pueden validar o desmentir reportes.

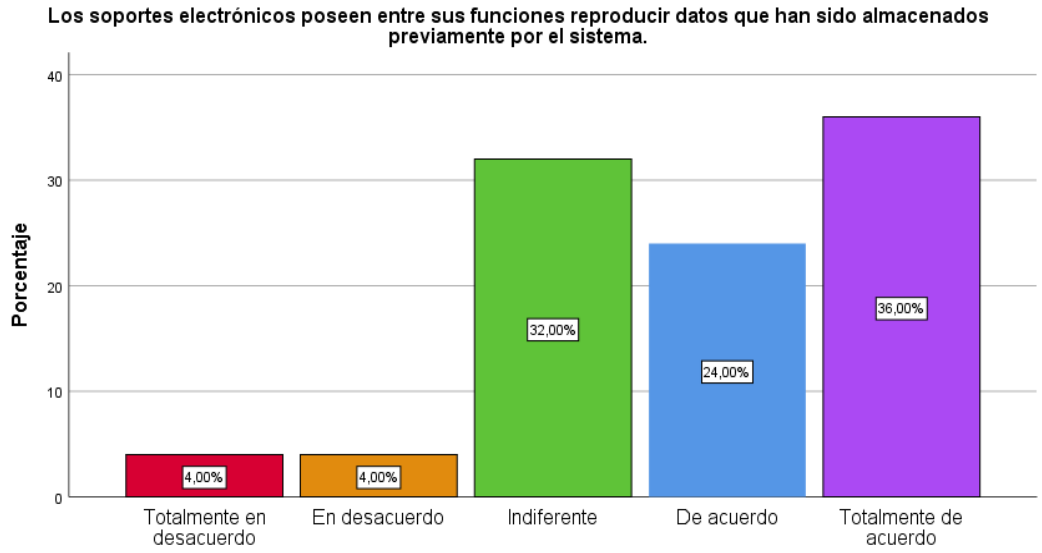
Tabla 31

Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	En desacuerdo	1	4,0	4,0	8,0
	Indiferente	8	32,0	32,0	40,0
	De acuerdo	6	24,0	24,0	64,0
	Totalmente de acuerdo	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Figura 12

Los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% totalmente de acuerdo en considerar que los soportes electrónicos poseen entre sus funciones reproducir datos que han sido almacenados previamente por el sistema.

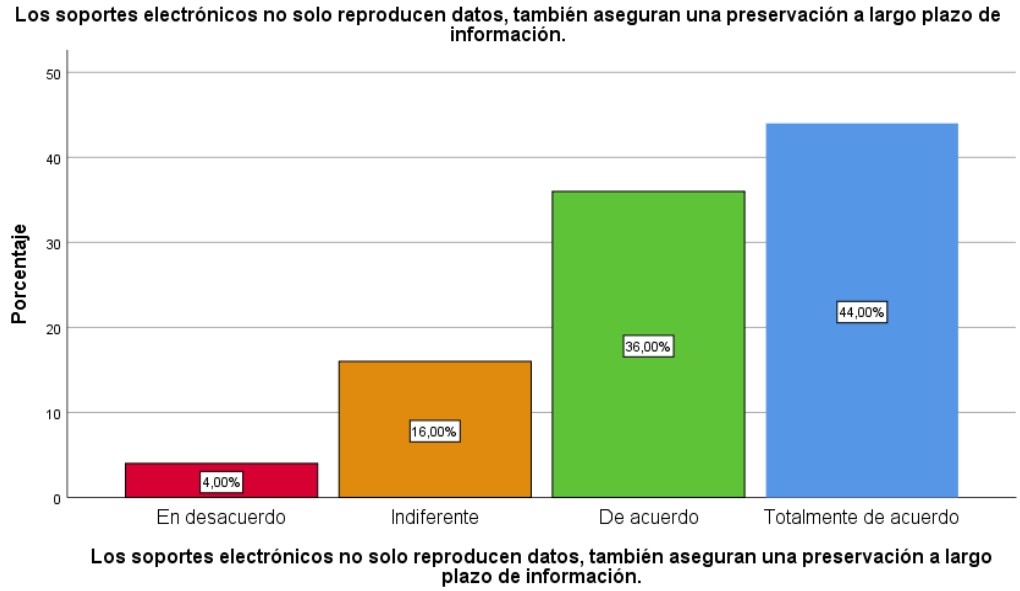
Tabla 32

Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	1	4,0	4,0	4,0
	Indiferente	4	16,0	16,0	20,0
	De acuerdo	9	36,0	36,0	56,0
	Totalmente de acuerdo	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Figura 13

Los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% totalmente de acuerdo en considerar que los soportes electrónicos no solo reproducen datos, también aseguran una preservación a largo plazo de información.

Tabla 33

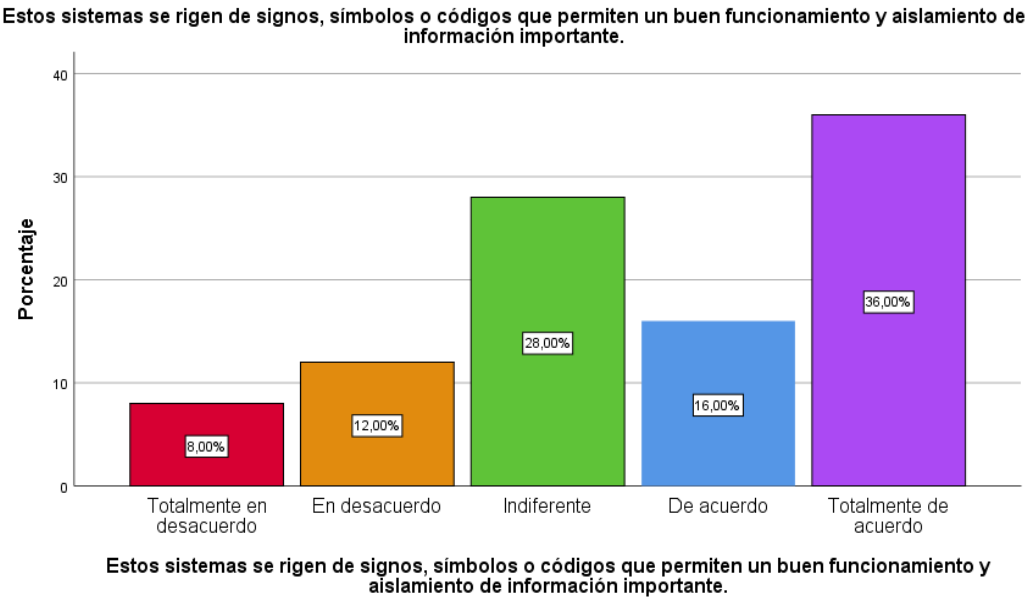
Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen

funcionamiento y aislamiento de información importante.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	3	12,0	12,0	20,0
	Indiferente	7	28,0	28,0	48,0
	De acuerdo	4	16,0	16,0	64,0
	Totalmente de acuerdo	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Figura 14

Estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% totalmente de acuerdo en considerar que estos sistemas se rigen de signos, símbolos o códigos que permiten un buen funcionamiento y aislamiento de información importante.

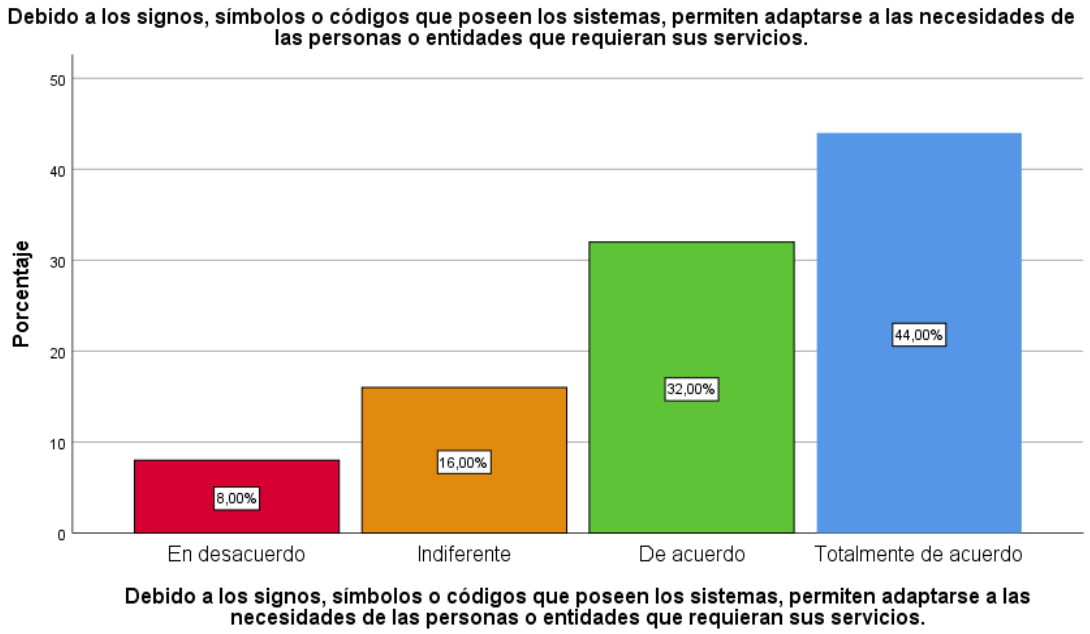
Tabla 34

Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	2	8,0	8,0	8,0
	Indiferente	4	16,0	16,0	24,0
	De acuerdo	8	32,0	32,0	56,0
	Totalmente de acuerdo	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Figura 15

Debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% totalmente de acuerdo en considerar que debido a los signos, símbolos o códigos que poseen los sistemas, permiten adaptarse a las necesidades de las personas o entidades que requieran sus servicios.

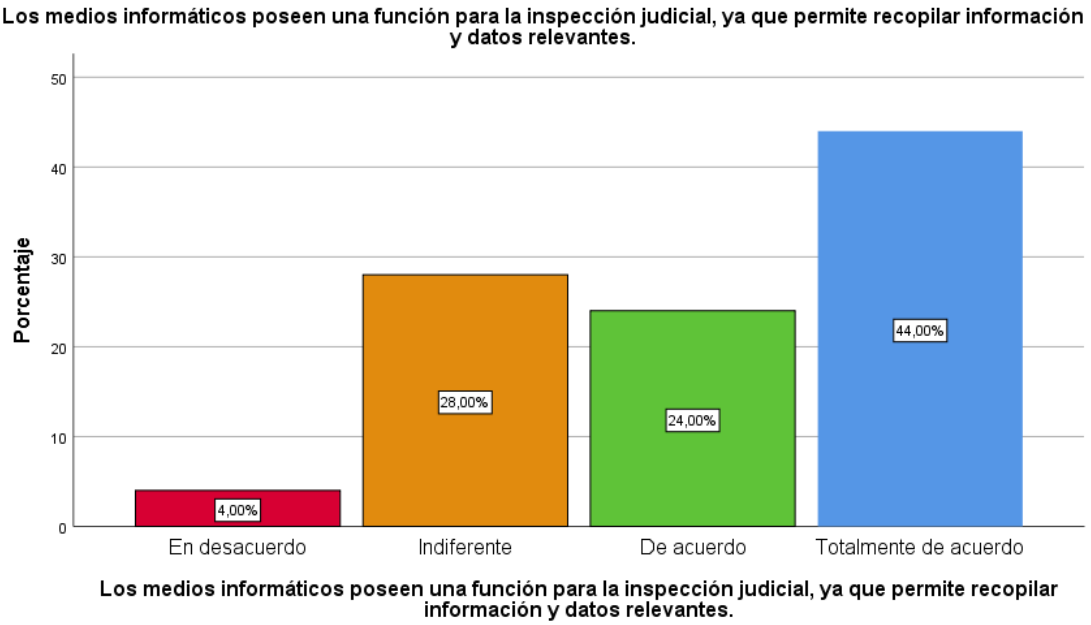
Tabla 35

Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	1	4,0	4,0	4,0
	Indiferente	7	28,0	28,0	32,0
	De acuerdo	6	24,0	24,0	56,0
	Totalmente de acuerdo	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Figura 16

Los medios informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% totalmente de acuerdo en considerar que los medios de informáticos poseen una función para la inspección judicial, ya que permite recopilar información y datos relevantes.

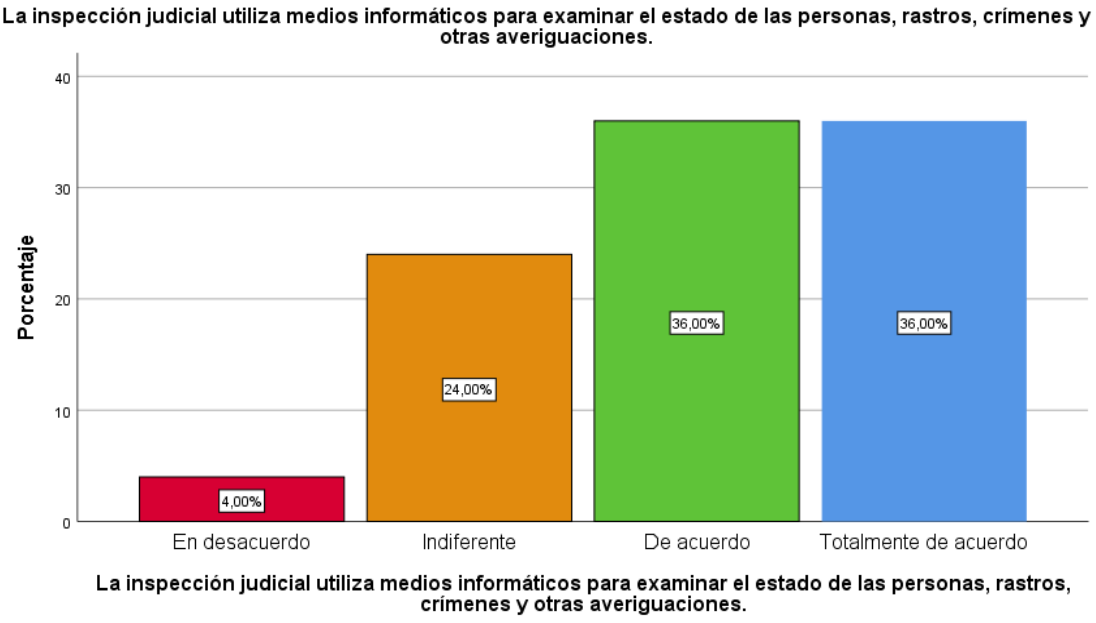
Tabla 36

La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	1	4,0	4,0	4,0
	Indiferente	6	24,0	24,0	28,0
	De acuerdo	9	36,0	36,0	64,0
	Totalmente de acuerdo	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Figura 17

La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.



La inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% tanto de acuerdo como totalmente de acuerdo en considerar que la inspección judicial utiliza medios informáticos para examinar el estado de las personas, rastros, crímenes y otras averiguaciones.

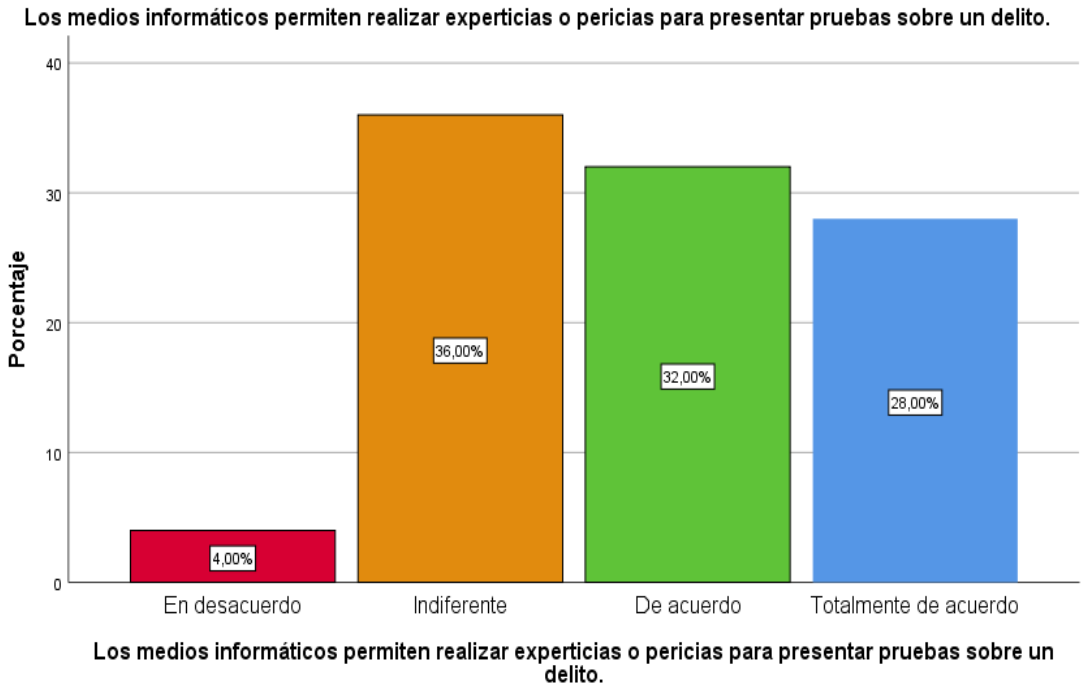
Tabla 37

Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	1	4,0	4,0	4,0
	Indiferente	9	36,0	36,0	40,0
	De acuerdo	8	32,0	32,0	72,0
	Totalmente de acuerdo	7	28,0	28,0	100,0
	Total	25	100,0	100,0	

Figura 18

Los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% indiferentes en considerar que los medios informáticos permiten realizar experticias o pericias para presentar pruebas sobre un delito.

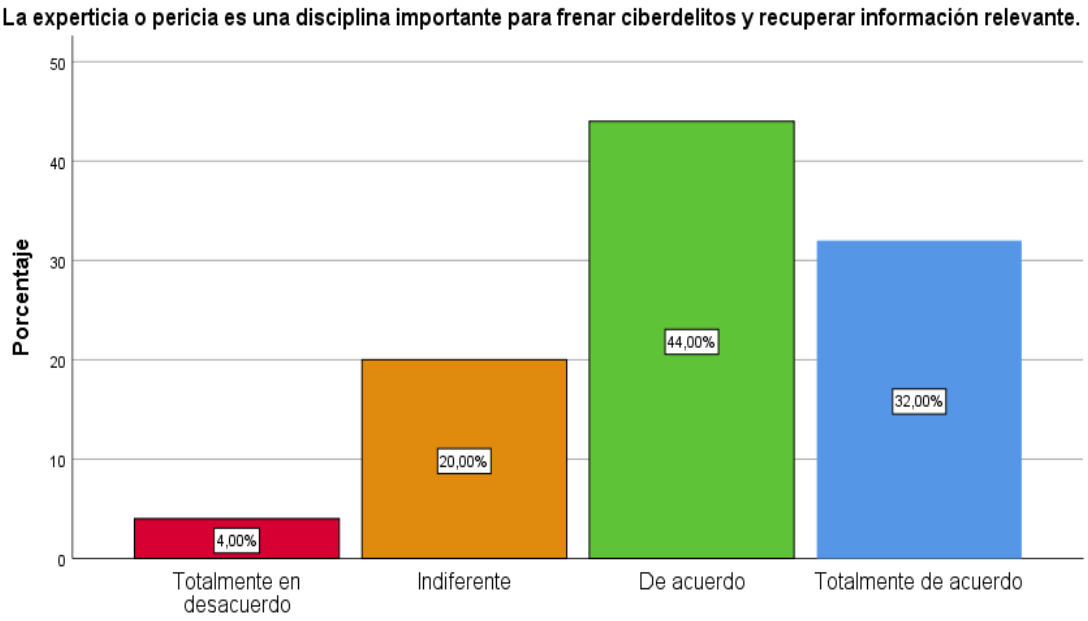
Tabla 38

La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	5	20,0	20,0	24,0
	De acuerdo	11	44,0	44,0	68,0
	Totalmente de acuerdo	8	32,0	32,0	100,0
	Total	25	100,0	100,0	

Figura 19

La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.



La experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% de acuerdo en considerar que la experticia o pericia es una disciplina importante para frenar ciberdelitos y recuperar información relevante.

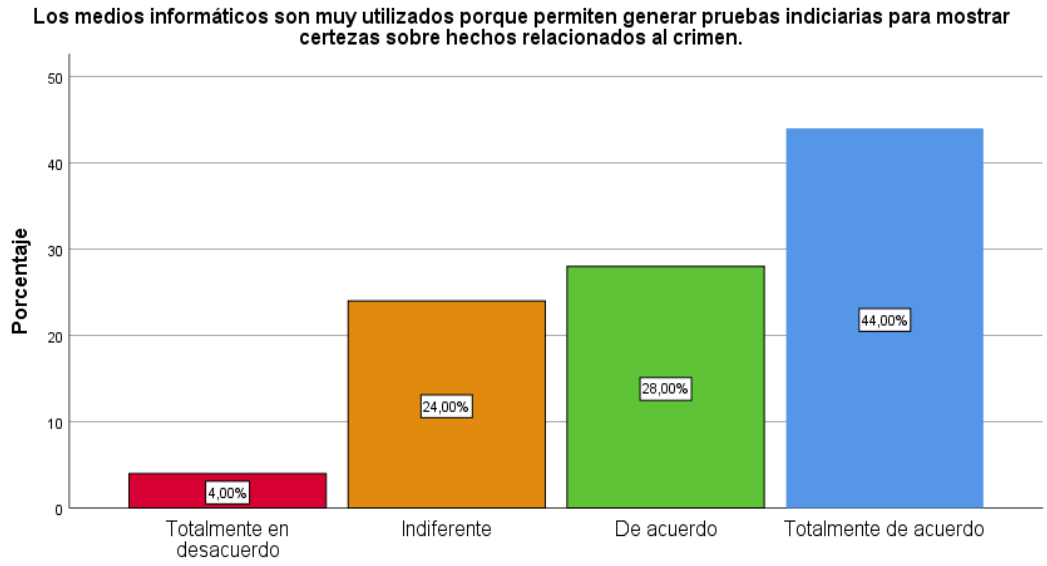
Tabla 39

Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	6	24,0	24,0	28,0
	De acuerdo	7	28,0	28,0	56,0
	Totalmente de acuerdo	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Figura 20

Los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% totalmente de acuerdo en considerar que los medios informáticos son muy utilizados porque permiten generar pruebas indiciarias para mostrar certezas sobre hechos relacionados al crimen.

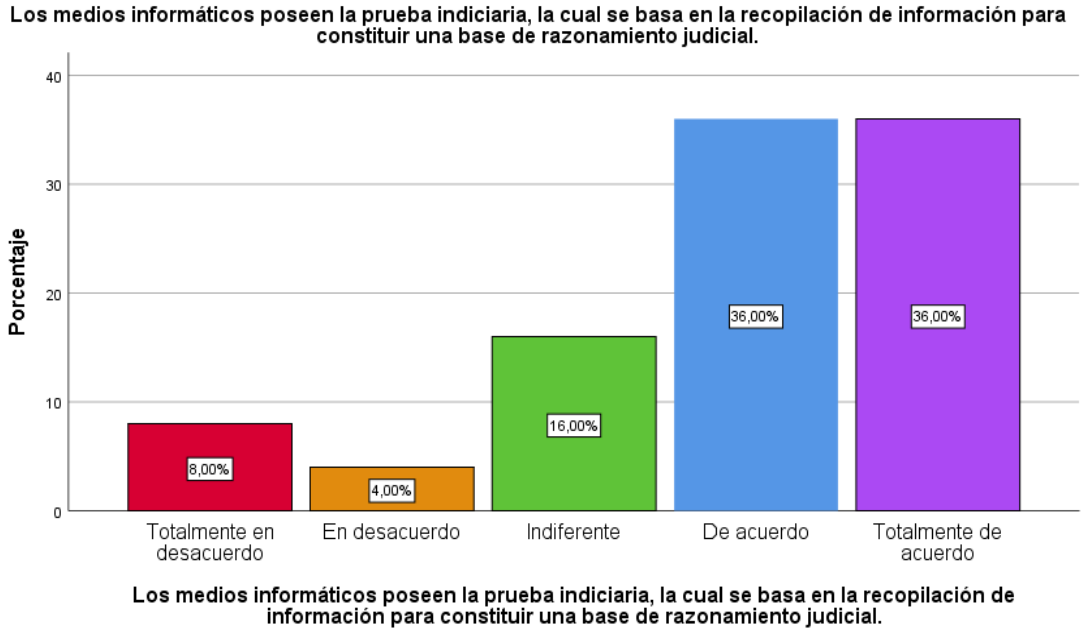
Tabla 40

Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	1	4,0	4,0	12,0
	Indiferente	4	16,0	16,0	28,0
	De acuerdo	9	36,0	36,0	64,0
	Totalmente de acuerdo	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Figura 21

Los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% tanto de acuerdo como totalmente de acuerdo en considerar que los medios informáticos poseen la prueba indiciaria, la cual se basa en la recopilación de información para constituir una base de razonamiento judicial.

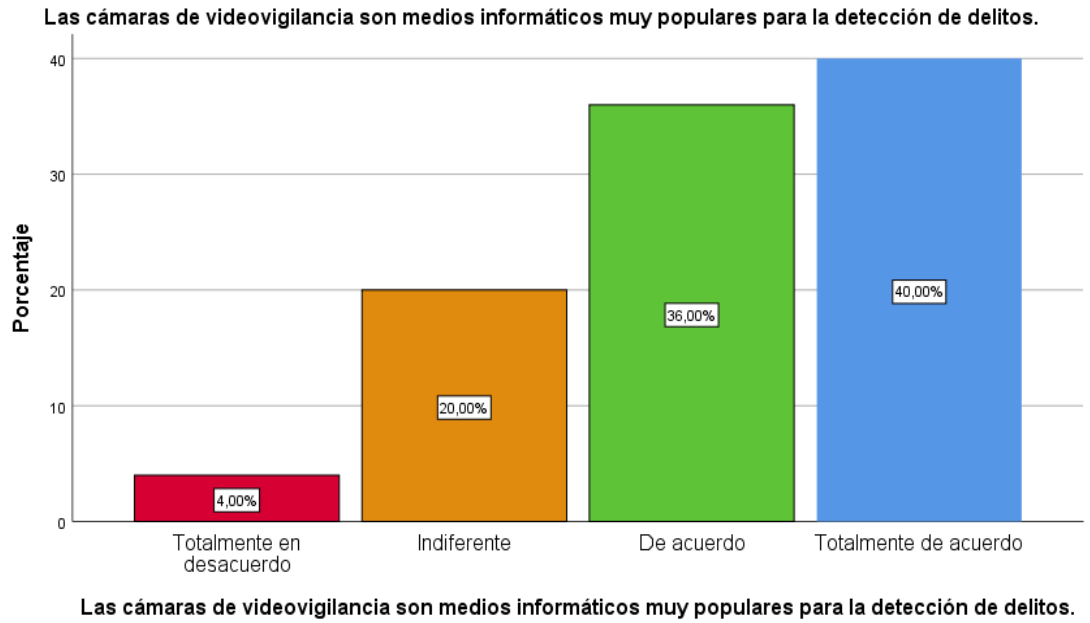
Tabla 41

Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	5	20,0	20,0	24,0
	De acuerdo	9	36,0	36,0	60,0
	Totalmente de acuerdo	10	40,0	40,0	100,0
	Total	25	100,0	100,0	

Figura 22

Las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 40.00% totalmente de acuerdo en considerar que las cámaras de videovigilancia son medios informáticos muy populares para la detección de delitos.

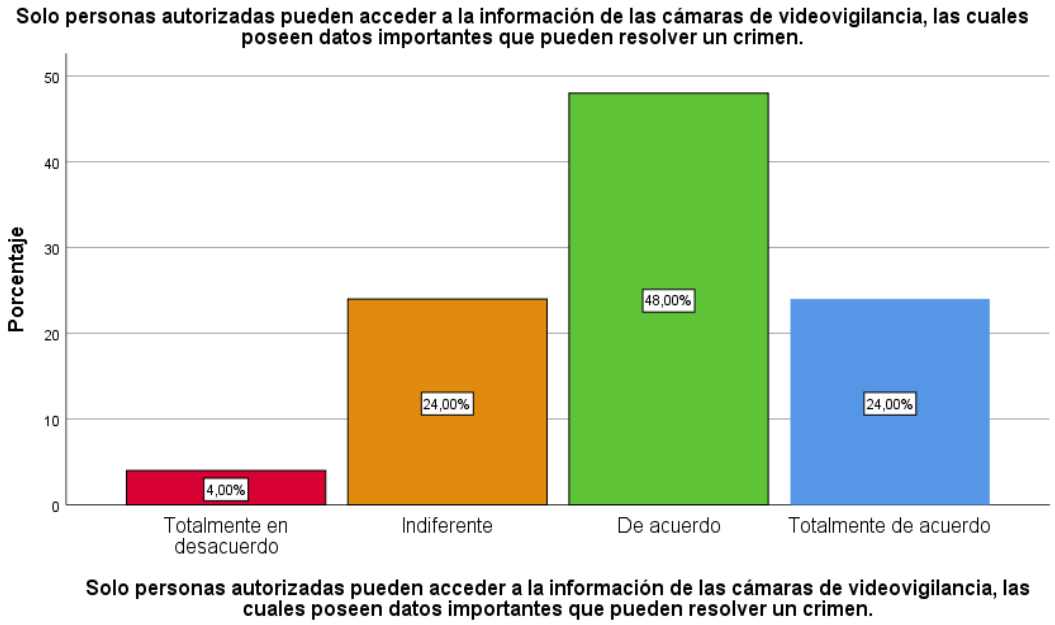
Tabla 42

Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	6	24,0	24,0	28,0
	De acuerdo	12	48,0	48,0	76,0
	Totalmente de acuerdo	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Figura 23

Solo personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 48.00% de acuerdo en considerar que solo las personas autorizadas pueden acceder a la información de las cámaras de videovigilancia, las cuales poseen datos importantes que pueden resolver un crimen.

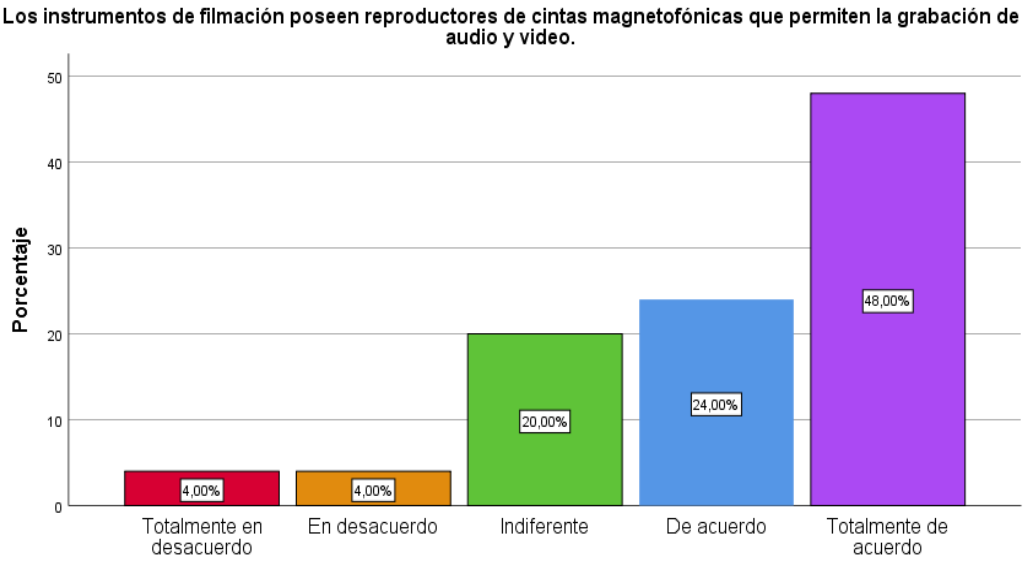
Tabla 43

Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	En desacuerdo	1	4,0	4,0	8,0
	Indiferente	5	20,0	20,0	28,0
	De acuerdo	6	24,0	24,0	52,0
	Totalmente de acuerdo	12	48,0	48,0	100,0
	Total	25	100,0	100,0	

Figura 24

Los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 48.00% totalmente de acuerdo en considerar que los instrumentos de filmación poseen reproductores de cintas magnetofónicas que permiten la grabación de audio y video.

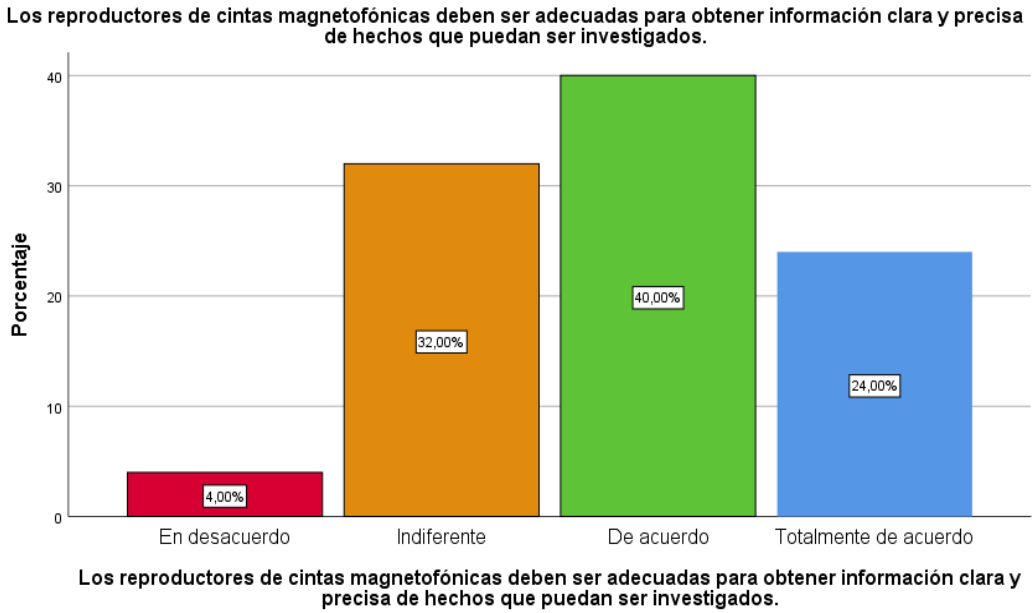
Tabla 44

Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	1	4,0	4,0	4,0
	Indiferente	8	32,0	32,0	36,0
	De acuerdo	10	40,0	40,0	76,0
	Totalmente de acuerdo	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Figura 25

Los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 40.00% de acuerdo en considerar que los reproductores de cintas magnetofónicas deben ser adecuadas para obtener información clara y precisa de hechos que puedan ser investigados.

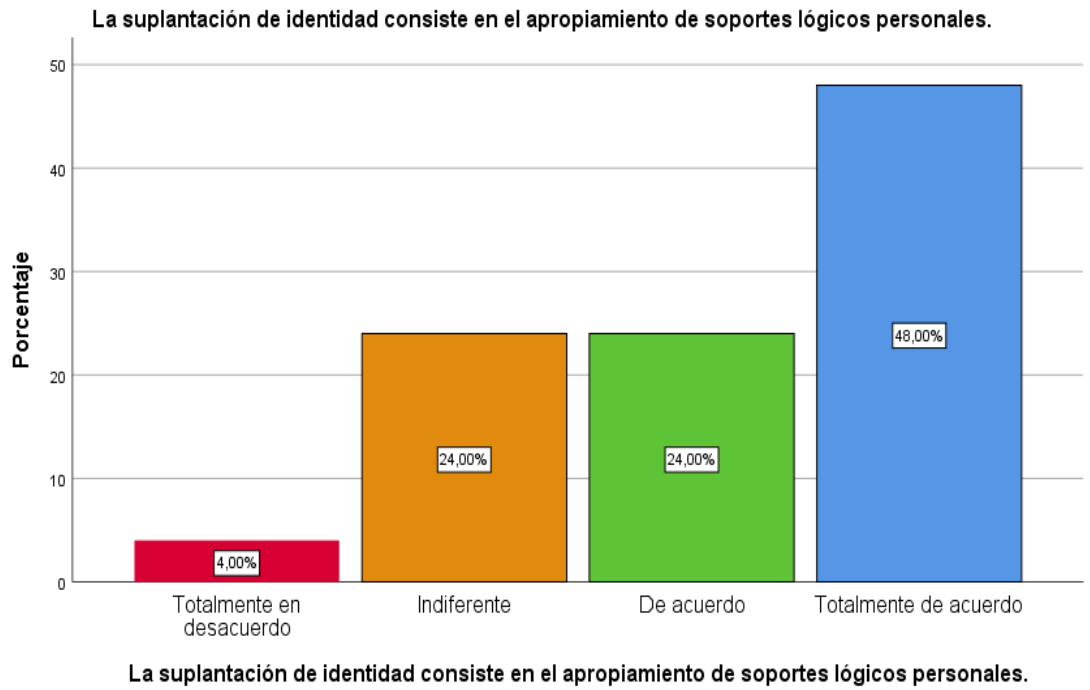
Tabla 45

La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	6	24,0	24,0	28,0
	De acuerdo	6	24,0	24,0	52,0
	Totalmente de acuerdo	12	48,0	48,0	100,0
	Total	25	100,0	100,0	

Figura 26

La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.



La suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 48.00% totalmente de acuerdo en considerar que la suplantación de identidad consiste en el apropiamiento de soportes lógicos personales.

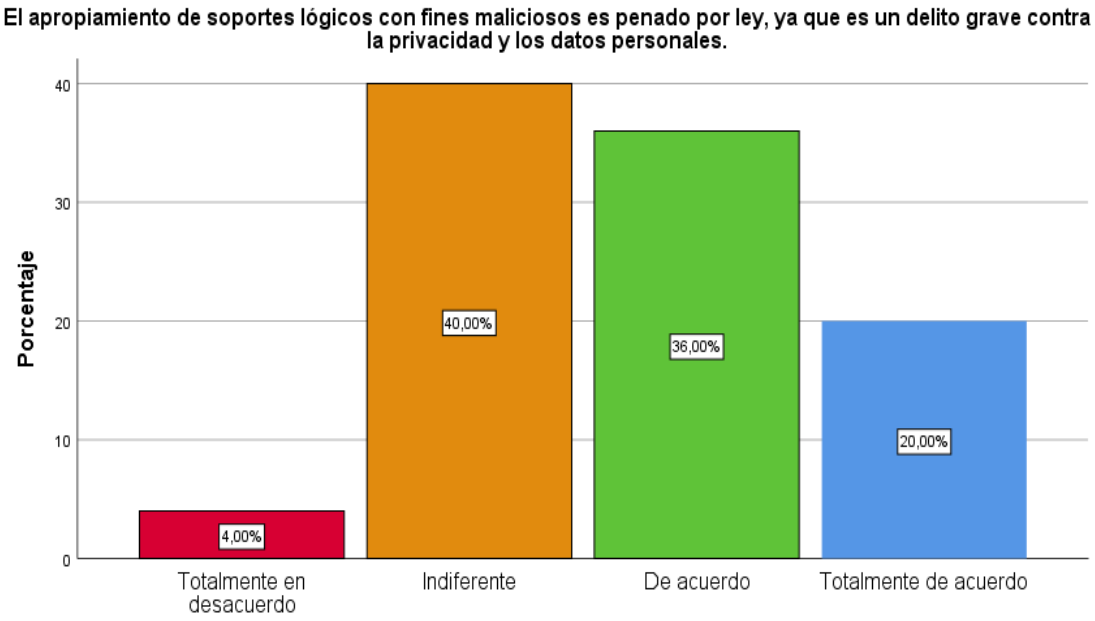
Tabla 46

El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	10	40,0	40,0	44,0
	De acuerdo	9	36,0	36,0	80,0
	Totalmente de acuerdo	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Figura 27

El apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos personales.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 40.00% indiferentes en considerar que el apropiamiento de soportes lógicos con fines maliciosos es penado por ley, ya que es un delito grave contra la privacidad y los datos

personales.

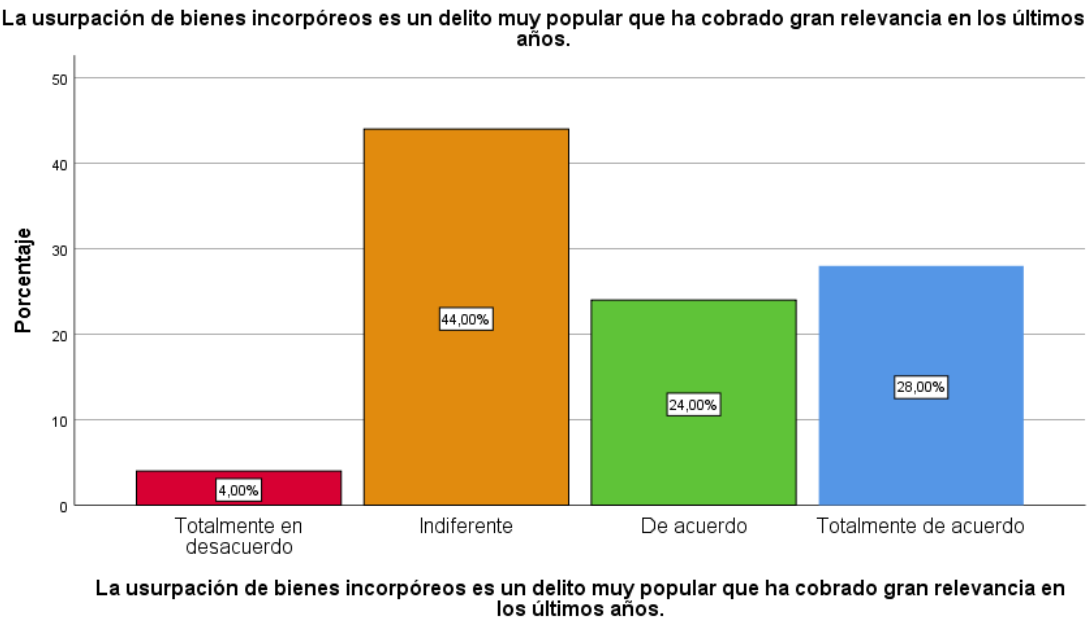
Tabla 47

La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	Indiferente	11	44,0	44,0	48,0
	De acuerdo	6	24,0	24,0	72,0
	Totalmente de acuerdo	7	28,0	28,0	100,0
	Total	25	100,0	100,0	

Figura 28

La usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% indiferentes en considerar que la usurpación de bienes incorpóreos es un delito muy popular que ha cobrado gran relevancia en los últimos años.

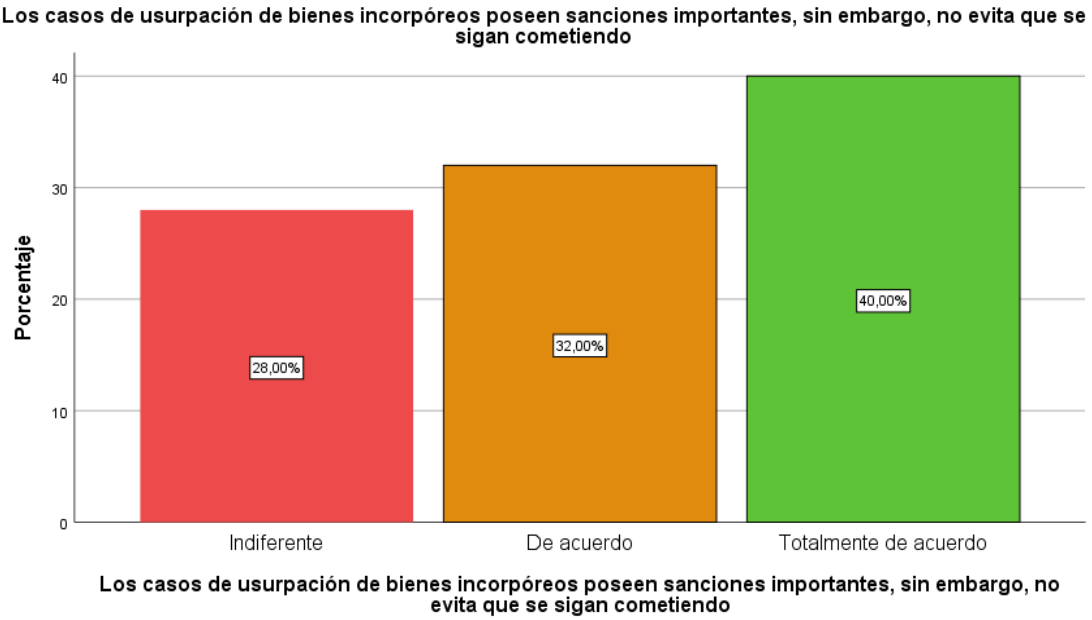
Tabla 48

Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Indiferente	7	28,0	28,0	28,0
	De acuerdo	8	32,0	32,0	60,0
	Totalmente de acuerdo	10	40,0	40,0	100,0
	Total	25	100,0	100,0	

Figura 29

Los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se siga cometiendo



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 40.00% totalmente de acuerdo en considerar que los casos de usurpación de bienes incorpóreos poseen sanciones importantes, sin embargo, no evita que se sigan cometiendo.

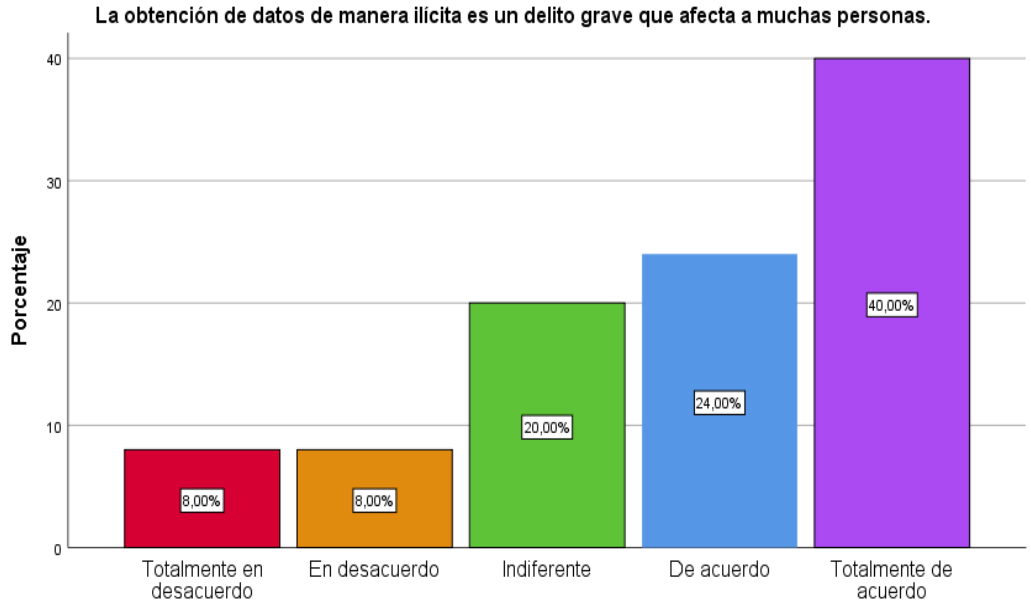
Tabla **49**

La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	2	8,0	8,0	16,0
	Indiferente	5	20,0	20,0	36,0
	De acuerdo	6	24,0	24,0	60,0
	Totalmente de acuerdo	10	40,0	40,0	100,0
	Total	25	100,0	100,0	

Figura 30

La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.



La obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 40.00% totalmente de acuerdo en considerar que la obtención de datos de manera ilícita es un delito grave que afecta a muchas personas.

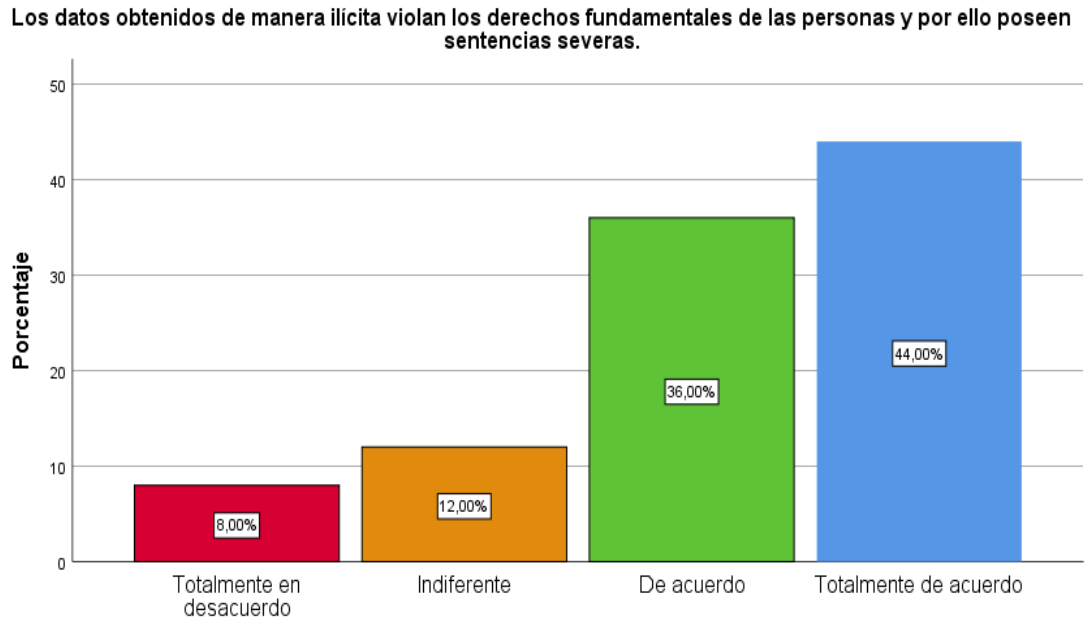
Tabla 50

Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	Indiferente	3	12,0	12,0	20,0
	De acuerdo	9	36,0	36,0	56,0
	Totalmente de acuerdo	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Figura 31

Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.



Los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% totalmente de acuerdo en considerar los datos obtenidos de manera ilícita violan los derechos fundamentales de las personas y por ello poseen sentencias severas.

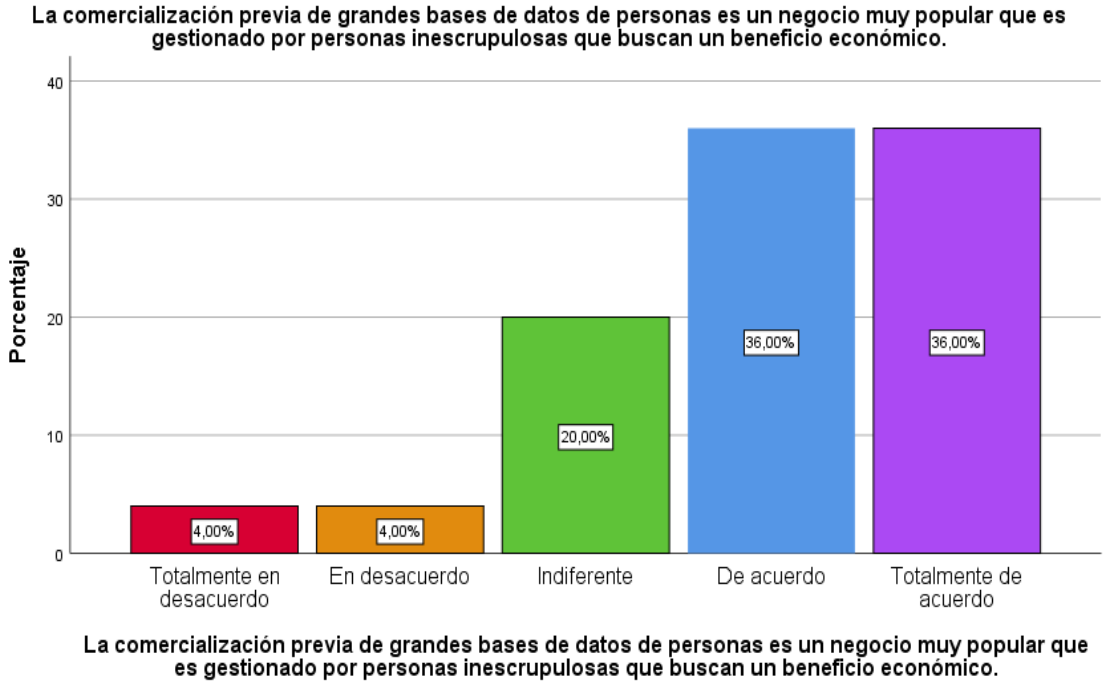
Tabla 51

La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	1	4,0	4,0	4,0
	En desacuerdo	1	4,0	4,0	8,0
	Indiferente	5	20,0	20,0	28,0
	De acuerdo	9	36,0	36,0	64,0
	Totalmente de acuerdo	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Figura 32

La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.



La comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% tanto

de acuerdo como totalmente de acuerdo en considerar que la comercialización previa de grandes bases de datos de personas es un negocio muy popular que es gestionado por personas inescrupulosas que buscan un beneficio económico.

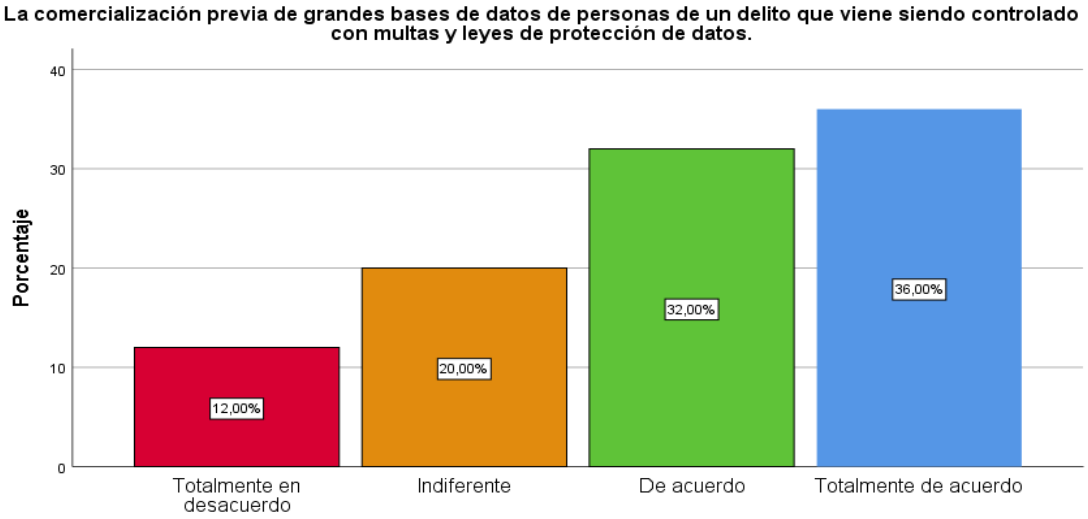
Tabla 52

La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	3	12,0	12,0	12,0
	Indiferente	5	20,0	20,0	32,0
	De acuerdo	8	32,0	32,0	64,0
	Totalmente de acuerdo	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Figura 33

La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.



La comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.

Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 36.00% totalmente de acuerdo en considerar que la comercialización previa de grandes bases de datos de personas de un delito que viene siendo controlado con multas y leyes de protección de datos.

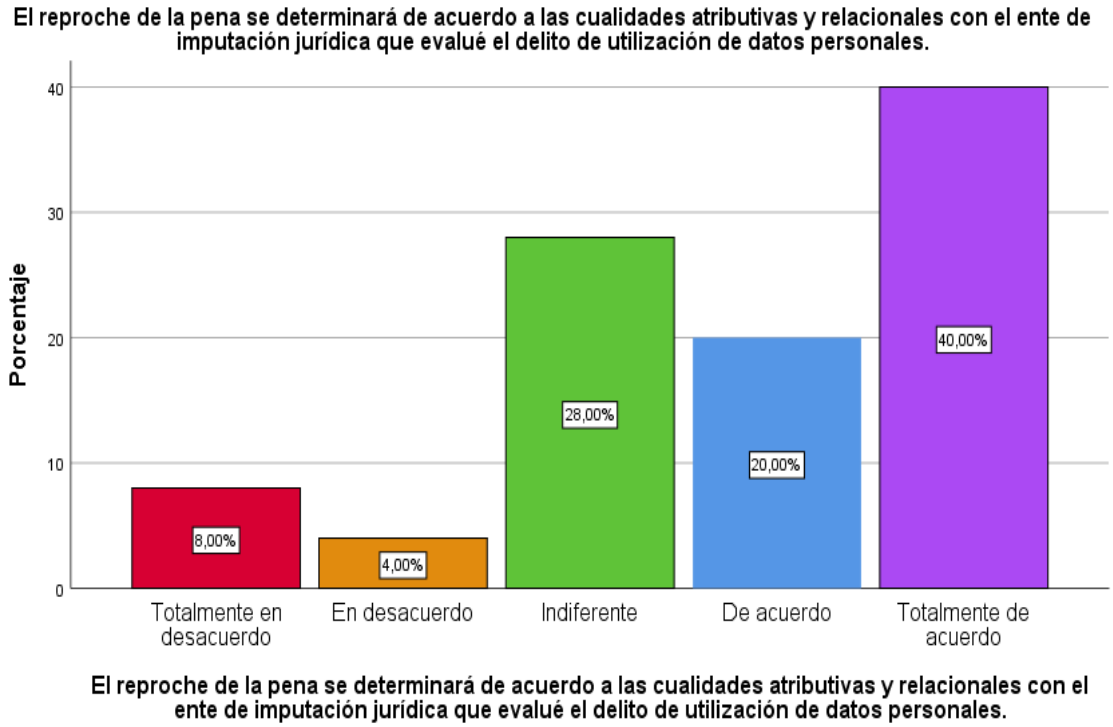
Tabla 53

El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	1	4,0	4,0	12,0
	Indiferente	7	28,0	28,0	40,0
	De acuerdo	5	20,0	20,0	60,0
	Totalmente de acuerdo	10	40,0	40,0	100,0
	Total	25	100,0	100,0	

Figura 34

El reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 40.00%

totalmente de acuerdo en considerar que el reproche de la pena se determinará de acuerdo a las cualidades atributivas y relacionales con el ente de imputación jurídica que evalué el delito de utilización de datos personales.

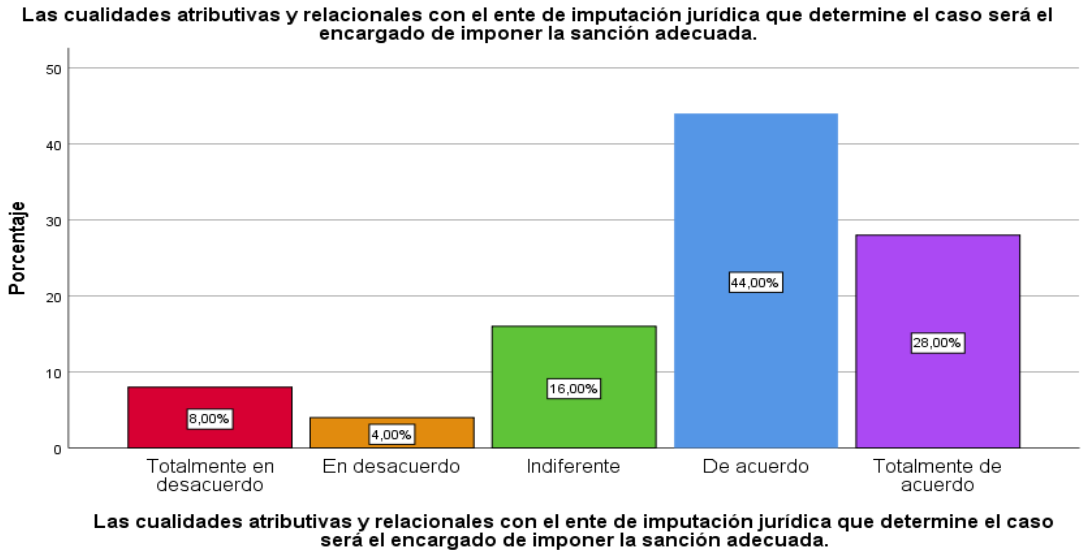
Tabla 54

*Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada***.**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	1	4,0	4,0	12,0
	Indiferente	4	16,0	16,0	28,0
	De acuerdo	11	44,0	44,0	72,0
	Totalmente de acuerdo	7	28,0	28,0	100,0
	Total	25	100,0	100,0	

Figura 35

Las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 44.00% de acuerdo en considerar que las cualidades atributivas y relacionales con el ente de imputación jurídica que determine el caso será el encargado de imponer la sanción adecuada.

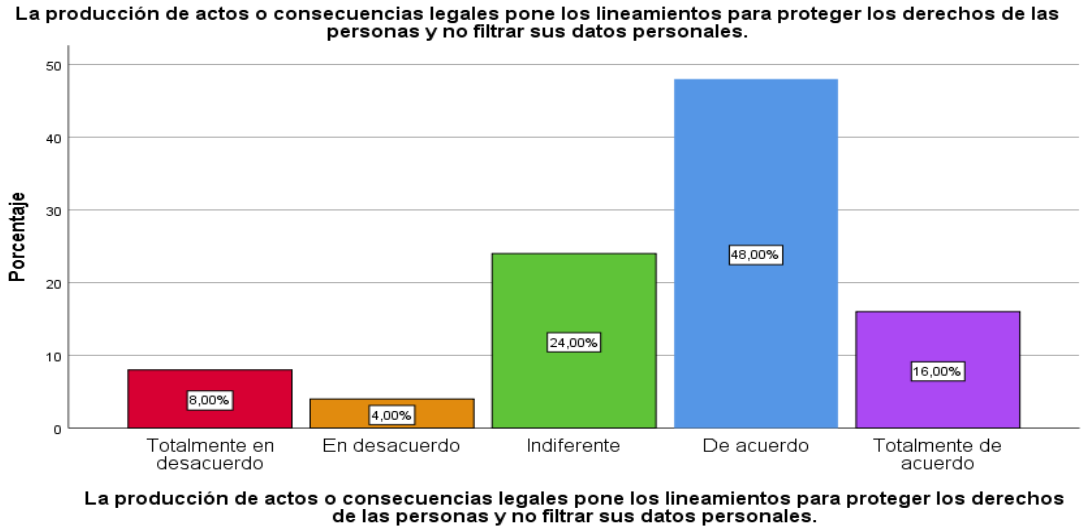
Tabla 55

La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	2	8,0	8,0	8,0
	En desacuerdo	1	4,0	4,0	12,0
	Indiferente	6	24,0	24,0	36,0
	De acuerdo	12	48,0	48,0	84,0
	Totalmente de acuerdo	4	16,0	16,0	100,0
	Total	25	100,0	100,0	

Figura 36

La producción de actos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 48.00% de acuerdo en considerar que la producción de datos o consecuencias legales pone los lineamientos para proteger los derechos de las personas y no filtrar sus datos personales.

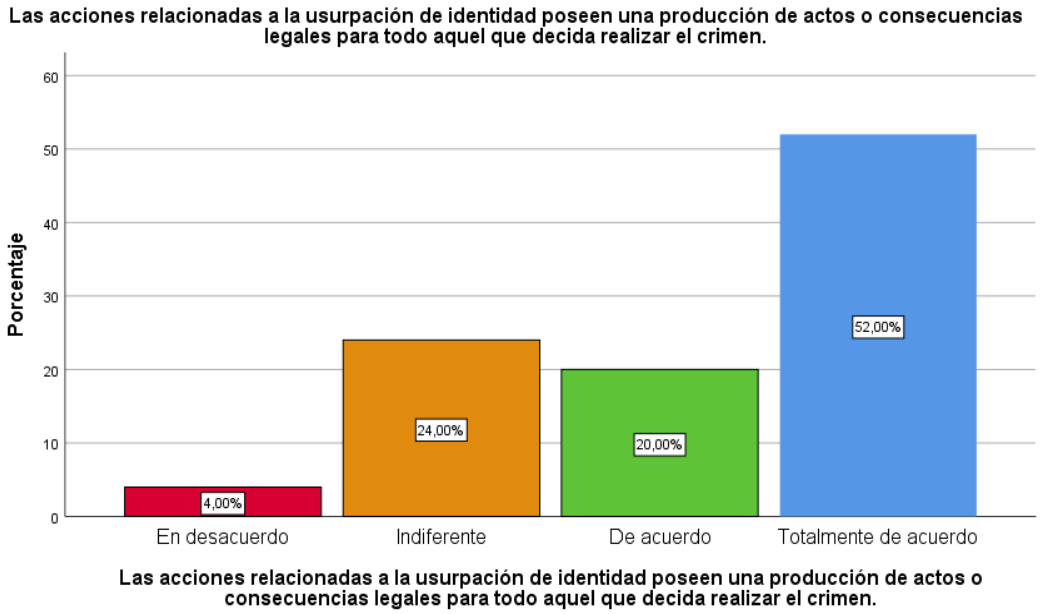
Tabla 56

Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En desacuerdo	1	4,0	4,0	4,0
	Indiferente	6	24,0	24,0	28,0
	De acuerdo	5	20,0	20,0	48,0
	Totalmente de acuerdo	13	52,0	52,0	100,0
	Total	25	100,0	100,0	

Figura 37

Las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.



Dentro de la tabla se pudo observar que entre los 25 efectivos policiales de la DIRINCRI especialistas en delitos informáticos encuestados estuvieron 52.00% totalmente de acuerdo en considerar que las acciones relacionadas a la usurpación de identidad poseen una producción de actos o consecuencias legales para todo aquel que decida realizar el crimen.

Anexo 6 Prueba de normalidad

Tabla 57

Prueba de normalidad – Medios informáticos.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Medios informáticos	,946	25	,207

En la variable Medios informáticos el <p valor> se considera mayor a 0,05 lo cual puede confirmar que la población es considerada normal lo que hace que se recurra a una prueba paramétrica.

Tabla 58

Prueba de normalidad – Delito de suplantación de identidad.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Delito de suplantación de identidad	,919	25	,064

En la variable Delito de suplantación de identidad el <p valor> se considera mayor a 0,05 lo cual puede confirmar que la población es considerada normal lo que hace que se recurra a una prueba paramétrica.

Anexo 7 Base de datos

MEDIOS INFORMÁTICOS																DELITO DE SUPLANTACIÓN DE IDENTIDAD												
Soportes electrónicos						Formas de aportación de prueba						Instrumentos de filmación				Apropiación de datos por medios convencionales o informáticos				Transferencia o cesión de datos personales				Utilización de datos personales			
V1P1	V1P2	V1P3	V1P4	V1P5	V1P6	V1P7	V1P8	V1P9	V1P10	V1P11	V1P12	V1P13	V1P14	V1P15	V1P16	V2P1	V2P2	V2P3	V2P4	V2P5	V2P6	V2P7	V2P8	V2P9	V2P10	V2P11	V2P12
5	4	5	5	3	5	3	4	3	4	3	5	5	4	3	4	4	3	5	4	4	5	4	5	4	5	5	4
4	4	4	5	3	3	3	5	4	3	5	3	3	4	4	3	3	4	3	3	5	5	4	4	5	4	3	5
3	3	3	3	3	5	4	4	5	4	3	5	4	3	4	3	3	3	3	4	4	4	4	3	5	5	4	5
4	5	3	5	3	5	3	4	4	5	5	5	5	5	3	3	5	4	4	5	4	5	3	5	3	5	3	5
5	4	4	3	5	5	5	5	5	4	4	4	5	5	5	5	4	3	5	5	3	5	5	3	3	5	3	5
3	4	3	4	3	5	4	3	4	5	4	5	4	3	3	4	3	3	3	5	5	3	4	4	4	4	4	5
3	4	5	4	5	4	3	3	3	4	5	3	4	5	4	5	5	3	4	4	3	5	5	3	4	3	4	5
5	4	3	4	4	4	5	3	3	3	3	4	4	3	4	3	5	4	5	5	5	5	4	5	3	4	3	5
3	4	4	5	4	5	5	5	3	4	3	4	3	3	5	3	5	5	3	3	3	5	4	4	5	3	3	4
4	5	3	4	5	3	5	4	3	5	3	4	5	5	5	4	3	3	4	5	4	4	5	3	3	5	5	4
5	3	5	5	3	5	4	3	3	3	3	4	4	4	3	5	3	3	3	5	5	4	5	3	3	3	4	3
3	3	4	3	3	4	5	5	3	4	4	3	4	4	5	4	4	4	4	5	5	4	3	5	5	4	3	5
5	5	3	5	5	5	5	4	5	4	5	5	3	4	5	4	4	4	3	3	3	4	5	5	4	4	4	4
3	3	5	4	5	5	4	3	3	5	5	5	3	5	5	3	5	5	3	3	3	3	5	4	3	4	5	3
3	3	4	4	4	3	5	3	4	5	4	4	5	4	3	4	5	5	3	5	5	4	3	4	5	5	5	5
4	4	5	5	5	4	4	5	4	4	5	4	4	4	5	4	5	4	4	4	4	5	4	5	5	4	4	5
4	5	5	5	5	4	4	5	5	5	4	5	5	4	5	4	5	5	5	4	5	5	5	5	5	4	4	5
4	4	5	4	5	5	5	5	5	5	5	4	5	5	5	5	4	4	5	4	4	4	4	4	5	5	4	5
4	4	5	4	4	4	5	4	4	4	5	5	5	4	5	4	5	5	5	5	5	5	4	4	5	4	4	4

5	4	5	4	5	4	5	5	4	5	4	5	4	4	4	5	4	4	4	5	5	4	5	5	4	4	4	5
1	3	1	2	2	4	3	5	2	1	1	1	4	3	5	2	3	3	3	4	1	1	2	5	3	3	2	3
3	2	3	5	2	5	2	2	3	4	5	1	5	4	5	5	5	3	3	3	2	4	5	1	5	1	1	3
2	5	2	3	1	2	3	4	4	3	5	3	3	1	1	4	1	3	3	3	1	5	3	1	2	1	1	2
1	2	4	5	1	3	5	4	5	4	5	2	1	3	4	3	5	4	1	4	2	1	3	1	1	2	4	3
4	4	3	5	2	2	3	4	5	3	4	4	5	4	2	3	5	1	5	3	5	3	1	4	1	4	4	3