



Universidad Nacional José Faustino Sánchez Carrión

Facultad de Derecho y Ciencias Políticas

Escuela Profesional de Derecho y Ciencias Políticas

**Delitos informáticos y la vulneración al derecho a la intimidad personal en la Provincia de
Barranca, 2023**

Tesis

Para optar el Título Profesional de Abogado

Autor

Pablo Emilio Vesga Guedes

Asesor

Mtro. Oscar Alberto Bailón Osorio

Huacho – Perú

2024



Reconocimiento - No Comercial – Sin Derivadas - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Reconocimiento: Debe otorgar el crédito correspondiente, proporcionar un enlace a la licencia e indicar si se realizaron cambios. Puede hacerlo de cualquier manera razonable, pero no de ninguna manera que sugiera que el licenciante lo respalda a usted o su uso. **No Comercial:** No puede utilizar el material con fines comerciales. **Sin Derivadas:** Si remezcla, transforma o construye sobre el material, no puede distribuir el material modificado. **Sin restricciones adicionales:** No puede aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros de hacer cualquier cosa que permita la licencia.



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020)

“AÑO DEL BICENTENARIO, DE LA CONSOLIDACIÓN DE NUESTRA INDEPENDENCIA, Y DE LA
CONMEMORACIÓN DE LAS HEROICAS BATALLAS DE JUNÍN Y AYACUCHO”

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO Y CIENCIAS POLÍTICAS

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	DNI	FECHA DE SUSTENTACIÓN
Pablo Emilio Vesga Guedes	42950091	29/12/2023
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	DNI	CÓDIGO ORCID
Oscar Alberto Bailón Osorio	31663048	0000-0002-7294-3548
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA- DOCTORADO:		
APELLIDOS Y NOMBRES	DNI	CODIGO ORCID
Silvio Miguel Rivera Jimenez	15724463	0000-0002-7293-4182
Jaime Andres Rodriguez Carranza	18071883	0000-0003-4101-2801
Elsa Silva Castro	09907053	0000-0003-1616-8898

Delitos informáticos y la vulneración al derecho a la intimidad personal en la provincia de Barranca, 2023

INFORME DE ORIGINALIDAD



FUENTES PRIMARIAS

1	repositorio.utelesup.edu.pe Fuente de Internet	<1 %
2	Submitted to Universidad Andina Nestor Caceres Velasquez Trabajo del estudiante	<1 %
3	repositorio.uigv.edu.pe Fuente de Internet	<1 %
4	shangay.com Fuente de Internet	<1 %
5	Submitted to Universidad Señor de Sipan Trabajo del estudiante	<1 %
6	suam.cucsh.udg.mx Fuente de Internet	<1 %
7	Submitted to uncedu Trabajo del estudiante	<1 %
8	hdl.handle.net Fuente de Internet	<1 %

TÍTULO

**“DELITOS INFORMÁTICOS Y LA
VULNERACIÓN A LA INTIMIDAD
PERSONAL EN LA PROVINCIA DE
BARRANCA, 2023”**

Autor: PABLO EMILIO VESGA GUEDES

Asesor: Mtro. Oscar Alberto Bailón Osorio

Universidad Nacional José Faustino Sánchez Carrión
Facultad de Derecho y Ciencias Políticas
Escuela Profesional de Derecho

JURADO EVALUADOR

Dr. SILVIO MIGUEL RIVERA JIMENEZ

Presidente

MG. JAIME ANDRES RODRIGUEZ CARRANZA

Secretario

DRA. ELSA SILVA CASTRO

Vocal

Mtro. OSCAR ALBERTO BAILON OSORIO

Asesor

DEDICATORIA

Se lo dedico a mi madre que desde el cielo sigue bendiciendo mi camino de vida y profesional; a mi Padrino Kike y mi tía Genoveva, que dieron todo por mí y fueron los que me impulsaron a poder estudiar de Derecho y Ciencias Políticas; y de forma especial a mi esposa Herlinda Ruiz, quien me estimuló a culminar mis estudios, quedando pocos peldaños para alcanzar mi Licenciatura.

Pablo Emilio Vesga Guedes

AGRADECIMIENTO

Agradezco a cada una de las personas que hicieron posible mi formación profesional, a mis docentes, a la universidad, a mis amigos que a pesar de todo los estimo, especialmente a mi esposa.

Pablo Emilio Vesga Guedes

ÍNDICE

DEDICATORIA	vii
AGRADECIMIENTO	viii
RESUMEN	xiii
ABSTRACT	xiv
INTRODUCCIÓN	xv
CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA	1
1.1. Descripción de la realidad problemática	1
1.2. Formulación del problema	3
1.2.1. Problema general	3
1.2.2. Problemas específicos	3
1.3. Objetivos de la investigación	3
1.3.1. Objetivo general	3
1.3.2. Objetivos específicos	3
1.4. Justificación de la investigación	4
1.5. Delimitaciones del estudio	5
1.6. Viabilidad del estudio	6
CAPITULO II. MARCO TEÓRICO	7
2.1. Antecedentes de la investigación	7
2.1.1. Investigaciones internacionales	7
2.1.2. Investigaciones nacionales	9
2.2. Bases teóricas	11
2.3. Bases Filosóficas	16
2.4. Definiciones de términos básicos	17
2.5. Hipótesis de investigación	18
2.5.1. Hipótesis general	18
2.6. Operacionalización de las variables	18

CAPÍTULO III. METODOLOGÍA	20
3.1. Diseño de la investigación	20
3.2. Población y muestra	21
3.2.1. Población	21
3.2.2. Muestra	21
3.3. Técnicas de recolección de datos	23
3.4. Técnicas para el procesamiento de la información	25
3.5. Matriz de consistencia	26
CAPÍTULO IV. RESULTADOS	27
4.1. Análisis de resultados	27
4.2. Contrastación de hipótesis	40
CAPÍTULO V	45
DISCUSIÓN	45
5.1. Discusión de resultados	45
CAPÍTULO VI	47
CONCLUSIONES Y RECOMENDACIONES	47
6.1. Conclusiones	47
6.2. Recomendaciones	48
REFERENCIAS	49
7.1. Fuentes documentales	49
7.2. Fuentes bibliográficas	51
7.3. Fuentes hemerográficas	52
7.4. Fuentes electrónicas	53
ANEXOS	54
Anexo 1: Matriz de consistencia	55
Anexo 2: Instrumentos	56
Anexo 3: Confiabilidad de los instrumentos	62
Anexo 4: Base de datos	63
Anexo 5: Evidencia fotográfica	64

ÍNDICE DE TABLAS

Tabla 1. Categoría de los delitos informáticos	27
Tabla 2. Categoría del derecho a la intimidad personal	28
Tabla 3. Listas de especialistas	30
Tabla 4. Pregunta 1	31
Tabla 5. Pregunta 2	32
Tabla 6. Pregunta 3	33
Tabla 7. Pregunta 4	34
Tabla 8. Pregunta 5	35
Tabla 9. Pregunta 6	35
Tabla 10. Pregunta 7	36
Tabla 11. Pregunta 8	37
Tabla 12. Pregunta 9	38
Tabla 13. Pregunta 10	39
Tabla 14. Pregunta 11	39
Tabla 15. Pregunta 12	40
Tabla 16. Prueba de Normalidad de delitos informáticos	41
Tabla 17. Prueba de Normalidad de derecho a la intimidad personal	42
Tabla 18. Correlación entre los delitos informáticos (DI) y Derecho a la intimidad personal (DIP)	44

ÍNDICE DE FIGURAS

Figura 1. Categoría de los delitos informáticos	27
Figura 2. Categoría del derecho a la intimidad personal	29
Figura 3. Histograma y curva normal de delitos informáticos	41
Figura 4. Histograma y curva normal de derecho a la intimidad personal	43

RESUMEN

Objetivo: El propósito de este estudio es evaluar el impacto de los delitos informáticos relacionados con los datos en la vulneración del derecho a la intimidad personal en la provincia de Barranca durante el año 2023. **Metodología:** Para llevar a cabo esta investigación, se empleó un enfoque cuantitativo de tipo aplicado, con un nivel correlacional-descriptivo. Se utilizó un diseño no experimental de corte transversal. La muestra consistió en 52 participantes. Se aplicó un cuestionario con 12 ítems en formato Likert para evaluar las variables de delitos informáticos y derecho a la intimidad personal. Además, se utilizó una guía de entrevista con 12 ítems. **Resultados:** Los resultados revelaron que el 72.7% de los encuestados siguen prácticas destinadas a prevenir los delitos informáticos, lo que contribuye a evitar ser víctimas de estos actos ilícitos. Además, el 77.3% de los participantes considera que la vulneración del derecho a la intimidad personal es de alta categoría. Las opiniones recopiladas a través de las entrevistas con especialistas también concuerdan en que los delitos informáticos tienen un impacto en la vulneración del derecho a la intimidad personal. Estos hallazgos se respaldan mediante una prueba de correlación positiva alta de Pearson, con un valor de 0.769, lo que demuestra la relación significativa entre ambas variables de estudio. **Conclusión:** En resumen, los resultados indican que los delitos informáticos relacionados con los datos tienen un impacto significativo en la vulneración del derecho a la intimidad personal en la provincia de Barranca durante el año 2023.

Palabras clave: Delitos informáticos, derecho a la intimidad personal, vulneración de derechos a la intimidad personal.

ABSTRACT

Objective: The primary aim of this study is to assess the impact of cybercrimes involving data on the infringement of individuals' right to personal privacy in the province of Barranca during the year 2023. **Methodology:** Employing a quantitative approach of the applied nature, with a correlational-descriptive level, this research adopted a non-experimental cross-sectional design. A sample of 52 participants was surveyed, employing a 12-item Likert scale questionnaire to evaluate the variables related to cybercrimes and the right to personal privacy. Additionally, a 12-item interview guide was employed. **Results:** The findings indicated that 72.7% of the survey participants follow practices geared towards the prevention of cybercrimes, reducing their susceptibility to such illicit activities. Furthermore, 77.3% of the respondents considered the violation of the right to personal privacy to be of a high magnitude. Insights gathered from interviews with specialists consistently supported the notion that cybercrimes have a substantial impact on the breach of the right to personal privacy. These findings were further substantiated by a Pearson correlation test showing a significantly high positive correlation of 0.769, thus establishing a meaningful relationship between the two study variables. **Conclusion:** In summary, this study concludes that cybercrimes involving data play a pivotal role in the infringement of the right to personal privacy in the province of Barranca in the year 2023.

Keywords: Computer crimes, right to personal privacy, violation of rights to personal privacy.

INTRODUCCIÓN

El presente trabajo de tesis, titulado "Delitos informáticos y su impacto en la vulneración del derecho a la intimidad personal en la provincia de Barranca en 2023," tuvo como propósito principal evaluar cómo los delitos informáticos afectan el derecho a la intimidad personal en la provincia de Barranca durante el año 2023.

Este trabajo se sustentó en el estudio de los delitos informáticos y sus componentes, como sistemas informáticos, datos informáticos y el acceso ilícito a los mismos. Además, se abordó el concepto del derecho a la intimidad personal, que engloba aspectos como la intimidad, la privacidad y la reserva. Las recomendaciones que se presentan en este estudio tienen como objetivo ayudar a los residentes de la provincia de Barranca a fortalecer su protección y prevenir la vulneración de su derecho a la intimidad personal, basándose en los resultados obtenidos.

La investigación se estructuró en seis capítulos de la siguiente manera:

Capítulo I: En este apartado se expondrá claramente la problemática, los objetivos de la investigación, la delimitación de las variables y la viabilidad del estudio.

Capítulo II: En este capítulo se respaldará el trabajo de investigación mediante investigaciones previas a nivel nacional e internacional que sustentan la base del estudio. Se explicará la conceptualización de las variables e indicadores y se presentará la hipótesis de investigación.

Capítulo III: En este apartado se detallará la metodología utilizada a lo largo de la investigación, incluyendo la población estudiada, la descripción de las variables, las técnicas y los instrumentos empleados en la recopilación y verificación de datos.

Capítulo IV: Aquí se presentará la selección y disposición de los resultados recopilados en campo. Estos se mostrarán en tablas y gráficos estadísticos, demostrando y validando la contrastación de hipótesis en la tesis.

Capítulo V: En este capítulo se expondrán los resultados junto con los antecedentes de investigación, lo que dará lugar a un análisis y discusión de los hallazgos.

Capítulo VI: En este apartado se presentarán las conclusiones y recomendaciones derivadas del trabajo de tesis.

Capítulo VII: Por último, se clasificarán las referencias bibliográficas siguiendo las pautas establecidas por la unidad de investigación de la universidad.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la actualidad, las técnicas de investigación se han convertido en una herramienta ampliamente utilizada a nivel global en diversas actividades cotidianas, priorizando el desarrollo y las necesidades individuales. Sin embargo, se ha observado un uso indebido de esta herramienta tecnológica en varios casos, resultando en la violación de los derechos fundamentales de las víctimas. En respuesta a esta problemática, varios estados han implementado procedimientos para salvaguardar estos derechos fundamentales.

Baño y Reyes (2020) señalan que las interacciones interpersonales, especialmente en entornos escolares, han transformado la forma en que las personas se comunican y trabajan con la información. Aunque esta herramienta es esencial para el contenido escolar, presenta deficiencias. En este sentido, es responsabilidad del Estado garantizar el disfrute adecuado de los derechos fundamentales, incluyendo la seguridad personal y familiar, la privacidad de la información y otros establecidos en la Constitución (p. 50).

Castro (2016) resalta la importancia de abordar el derecho a la seguridad de los residentes, especialmente en comunidades en línea, donde este derecho a menudo se pasa por alto (p. 34).

Desde la perspectiva de Jacobo y Quispe (2019), es fundamental educar a tutores, educadores y jóvenes sobre el uso de plataformas como Facebook y Twitter, ya que han

surgido preocupaciones, especialmente en cuanto a la seguridad de la información personal. Estas preocupaciones han llevado a propuestas de medidas de protección de la información personal y seguridad de datos en comunidades en línea (p. 9).

García (2015) destaca cómo la presencia de Internet y la diversidad de marcos computacionales han cambiado la forma en que las personas abordan los sistemas de datos y la comunicación, afectando todos los aspectos de la sociedad.

Palacios (2021) subraya que nuestro país no está exento de este creciente problema, donde los derechos fundamentales han sido violados mediante el robo de identidad, el robo virtual de información y la suplantación de identidad. Esto permite que los delincuentes se beneficien de estas actividades mediante el uso de tecnología avanzada. Además, se han desarrollado variantes de este delito, como el acceso ilegal a bases de datos almacenadas en sistemas informáticos, facilitando la comisión de otros delitos en el mercado negro. La delincuencia ha experimentado un aumento en la era de la globalización, trascendiendo las fronteras jurisdiccionales y las competencias locales (Urpeque, 2019).

El objetivo de este estudio fue evaluar el impacto de las infracciones de datos en la vulneración del derecho a la seguridad personal en la provincia de Barranca en 2023.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo los delitos informáticos contra los datos influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023?

1.2.2. Problemas específicos

- ¿Cómo los delitos informáticos contra los datos influyen en la vulneración de la intimidad personal en la provincia de Barranca en el año 2023?
- ¿Cómo los delitos informáticos contra los datos influyen en la vulneración de la privacidad personal en la provincia de Barranca en el año 2023?
- ¿Cómo los delitos informáticos contra los datos influyen en la vulneración de la reserva personal en la provincia de Barranca en el año 2023?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar la influencia de los delitos informáticos contra los datos sobre la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023.

1.3.2. Objetivos específicos

- Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la intimidad personal en la provincia de Barranca en el año 2023.
- Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la privacidad personal en la provincia de Barranca en el año 2023.

- Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la reserva personal en la provincia de Barranca en el año 2023.

1.4. Justificación de la investigación

Justificación teórica La fundamentación teórica de la presente investigación se apoya en la capacidad que ofrece para analizar los delitos informáticos y la vulneración del derecho a la intimidad personal. Estos aspectos sirvieron como base para la formulación de leyes. La relevancia de esta perspectiva radica en la comprensión, evolución, criterios y doctrinas vinculadas con la investigación, según las opiniones de diversos juristas.

Justificación práctica Esta investigación se concentra en abordar la problemática asociada con la detección, aplicación y sanción de los delitos informáticos, los cuales con frecuencia dejan a las víctimas en una posición vulnerable respecto a sus derechos fundamentales. Esto no solo impacta la privacidad personal, sino que también tiene consecuencias en su entorno. Por lo tanto, resulta esencial fortalecer las medidas en nuestra legislación penal y procesal penal para disminuir la incidencia de estos delitos.

Justificación social El propósito primordial de este trabajo de investigación jurídica es contribuir a la mejora de la legislación en nuestro país en lo que concierne a los delitos informáticos y la vulneración del derecho a la intimidad personal en nuestra sociedad.

Justificación metodológica Esta investigación se centra en la identificación de las variables de estudio, para las cuales se emplearán técnicas de encuesta y entrevista. Los instrumentos de recolección de datos consistirán en un cuestionario y una guía de entrevista, asignados a cada variable. Con el fin de

asegurar una recopilación de información efectiva, se han diseñado dos instrumentos, uno con 10 ítems para el cuestionario y otro con 12 ítems para la guía de entrevista. Esto posibilitará obtener resultados precisos en el desarrollo de la investigación.

1.5. Delimitaciones del estudio

Delimitación espacial Esta investigación se desarrolló en la Provincia de Barranca, la cual se encuentra ubicada en la Región Lima - Provincia.

Delimitación social El enfoque de la investigación se orientó a examinar las modificaciones legales y las sanciones vinculadas a los delitos informáticos, las cuales están sujetas a cambios continuos en nuestra sociedad debido a la constante evolución tecnológica experimentada por nuestros ciudadanos.

Delimitación temporal El estudio abarcó un periodo de tiempo específico durante el cual se recopiló información histórica y actual, antecedentes, fundamentos teóricos y teorías vinculadas con las variables de estudio. Posteriormente, se construyó una base de datos que contiene los resultados de la recopilación de información, permitiéndonos poner a prueba las hipótesis de investigación y llegar a las conclusiones de la tesis.

Delimitación conceptual Las propuestas formuladas para la realización de la indagación tenían como finalidad unificar y combinar conceptos y definiciones teóricas relacionadas con los delitos informáticos y el derecho a la intimidad personal bajo estudio.

1.6. Viabilidad del estudio

El proyecto de investigación cumplió con los criterios establecidos por la unidad de grados y títulos de la Facultad de Derecho y Ciencia Política, lo que nos proporcionó una comprensión más completa de las perspectivas y expectativas de nuestra nueva generación en lo que respecta al respeto a la intimidad personal.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Investigaciones internacionales

Amores (2022) llevó a cabo una investigación titulada "La ausencia de tipificación del delito informático 'sexting' dentro del COIP y su impacto en los derechos de la dignidad humana e intimidad en el Ecuador". Su objetivo era realizar un análisis jurídico, doctrinario y crítico de la falta de tipificación del delito de "sexting" en el Código Orgánico Integral Penal (COIP) y su repercusión en la dignidad humana y la intimidad personal. El estudio también propuso reformas al COIP que incluyeran la tipificación completa del delito de "sexting" junto con sanciones apropiadas. La investigación resaltó la falta de regulación del "sexting" en la legislación ecuatoriana, un problema en aumento debido al uso inapropiado de la tecnología, especialmente entre adolescentes y jóvenes. La metodología utilizada se basó en enfoques analíticos y sintéticos, respaldados por fuentes bibliográficas y documentales para fundamentar el marco teórico. Salvador (2022) desarrolló una investigación titulada "Derecho a la intimidad y ciberdelincuencia. Efectos sociales y económicos en víctimas ecuatorianas" con el propósito de describir el derecho a la intimidad y la ciberdelincuencia, así como sus consecuencias en las víctimas ecuatorianas. Se llevó a cabo un estudio cuantitativo de enfoque descriptivo y analítico, sin carácter experimental. El autor analizó la evolución y comportamiento de los delitos cibernéticos en Ecuador desde 2017 hasta 2021, con énfasis en 2020. Se emplearon técnicas documentales y análisis estadístico de los delitos informáticos proporcionados por el Sistema Integrado de Actuaciones Fiscales. Los resultados revelaron que los delitos

más frecuentes fueron la violación de la intimidad y la estafa. Cuñas (2021) focalizó su investigación en "Los datos personales en las redes sociales y el derecho a la intimidad personal", examinando la violación del derecho a la intimidad establecido en el artículo 178 del Código Orgánico Integral Penal a través de la red social Facebook. Este estudio combinó un análisis doctrinal y legal del derecho a la intimidad con un análisis de 13 casos de difusión de datos personales. Se utilizó una metodología cualitativa para examinar las fuentes consultadas y se llevó a cabo una encuesta entre abogados en ejercicio en la ciudad de Riobamba. Los resultados llevaron a la conclusión de que la incidencia de delitos en las redes sociales en Ecuador es baja, y que los delitos sancionados tienden a ser de poca gravedad, lo que dio lugar a propuestas y recomendaciones. Zamora (2020) realizó una investigación titulada "Los delitos informáticos y el derecho a la intimidad en el Código Orgánico Integral Penal", con el objetivo de realizar un análisis jurídico de los delitos informáticos, sus sanciones y su impacto en el derecho a la intimidad de las personas. El autor utilizó el método científico, recopiló información bibliográfica y documental, y llevó a cabo un estudio de campo que incluyó encuestas a abogados en ejercicio. Los resultados respaldaron la hipótesis de que los delitos informáticos afectan el derecho a la intimidad. Baño y Reyes (2020) en su investigación "Vulneración del derecho a la intimidad personal y familiar en las redes sociales" exploraron cómo el Estado garantiza los derechos fundamentales, incluyendo el derecho a la intimidad personal y familiar, a través de la Constitución. El estudio destacó que el uso inadecuado de las redes sociales puede dar lugar a delitos como secuestros, extorsiones, fraudes, acoso, intimidación, suplantación de identidad, uso de software malicioso y violación de la intimidad. Además, se resaltó la importancia de diferenciar el derecho a la intimidad de otros derechos fundamentales y se discutió cómo las

Tecnologías de la Información y la Comunicación pueden poner en peligro la integridad personal y social de los usuarios si se utilizan de manera inadecuada.

2.1.2. Investigaciones nacionales

En su estudio titulado "La vulneración del derecho a la intimidad", Zarate (2023) abordó la problemática de cómo se afecta el derecho a la intimidad personal. Por otro lado, el trabajo de "Autor X" (2021) titulado "Evaluación de la vulneración del derecho a la intimidad personal en los jóvenes en la Provincia de Bagua en el año 2021" tuvo como objetivo examinar en qué medida se comprometía el derecho a la intimidad personal de los jóvenes en la provincia de Bagua durante el año mencionado. La investigación se basó en una muestra de 70 jóvenes y utilizó métodos lógico-inductivos y deductivos, así como análisis descriptivos y analíticos. Se emplearon herramientas como formularios, cuestionarios, encuestas y guías de entrevista. Los resultados señalaron que el 45.71% de los participantes estuvo de acuerdo en la necesidad de establecer leyes que protejan la privacidad en línea, mientras que el 25.71% no compartió esa opinión, indicando una falta de conciencia sobre la importancia del problema. En resumen, el aumento de la suscripción a redes sociales y el consiguiente aumento de la compartición pública de información personal subraya la necesidad de leyes y protocolos más sólidos para abordar la privacidad en línea.

En su investigación "Los delitos informáticos y el derecho a la intimidad personal en Lima Metropolitana, 2021", Pérez (2022) se propuso analizar cómo los delitos informáticos impactan en el derecho a la intimidad personal en Lima Metropolitana durante 2021. El enfoque metodológico empleado fue cualitativo, con un diseño descriptivo y el análisis de artículos científicos indexados en bases de datos. Los

resultados se centraron en las definiciones de los delitos informáticos y su impacto en la intimidad de las personas. La conclusión fue que el avance tecnológico y la falta de educación en informática han dado lugar a delitos informáticos que afectan la intimidad personal, lo que requiere una modificación normativa y campañas de prevención para evitar la ingeniería social.

Aredo (2021) llevó a cabo la investigación "El phishing y su vulneración a la protección de datos personales en los delitos informáticos" con el objetivo de analizar si el phishing compromete la protección de datos personales en los delitos informáticos. La investigación se basó en un enfoque básico y descriptivo, con un análisis de documentos y una revisión de la literatura. Los resultados destacaron la necesidad de modificar la normativa para abordar el phishing y prevenir delitos informáticos. Se sugirió la implementación de mecanismos de autenticación y campañas de concienciación para prevenir la ingeniería social.

Palacios (2021) realizó una investigación titulada "Los Delitos Informáticos contra Datos, y su Vulneración al Derecho de la Intimidad Personal, en la Ciudad de Ayacucho, 2020". Su objetivo fue determinar cómo los delitos informáticos afectan el derecho a la intimidad personal en la ciudad de Ayacucho en 2020. La investigación se basó en un enfoque cualitativo y descriptivo, con la participación de 06 abogados. Los resultados resaltaron que los delitos informáticos contra datos claramente vulneran el derecho a la intimidad personal, lo que requiere una mayor atención y la adecuada aplicación de la normativa.

Finalmente, Jacobo y Quispe (2019) llevaron a cabo la investigación "Delitos informáticos orientados en casos de violación a la intimidad en el ámbito sexual de Lima Metropolitana-2018" con el objetivo de analizar cómo se establecen los delitos informáticos en casos de violación de la intimidad en el ámbito sexual en Lima

Metropolitana durante 2018. La metodología incluyó encuestas a personas que fueron víctimas de violación de la intimidad, con un enfoque doctrinario y legislativo. Los resultados destacaron que la violación de la intimidad es un delito de acción privada, lo que significa que no amenaza el orden comunitario, sino a una persona en particular, y que se requiere una intervención activa de las víctimas para denunciar estos delitos, similar a otros delitos como la injuria, difamación y calumnia.

2.2. Bases teóricas

2.2.1. Delitos informáticos

Los delitos informáticos, también conocidos como ciberdelitos o delitos cibernéticos, son acciones ilegales que aprovechan computadoras, sistemas de información, redes y tecnologías de la información para llevar a cabo actividades criminales. Estas actividades abarcan una amplia gama de acciones, que van desde el robo de datos personales hasta la alteración de servicios en línea, la perpetración de fraudes cibernéticos y diversos actos delictivos. Debido a la capacidad de los delincuentes informáticos para operar de manera global y anónima en el entorno digital, resulta especialmente difícil rastrear sus actividades. En respuesta a este desafío, numerosas jurisdicciones han promulgado legislación y regulaciones específicas para abordar estos delitos, y han establecido fuerzas de seguridad cibernética y equipos de respuesta a incidentes para prevenir y resolver los delitos informáticos. Además, es fundamental que las personas tomen medidas para proteger su seguridad y datos en línea, lo que implica el uso de contraseñas seguras y la adquisición de conocimientos sobre las amenazas cibernéticas.

2.2.1.1. Tráfico ilegal de datos

Mayer (2017) El tráfico ilegal de datos, conocido también como comercio o tráfico de información o datos robados, hace referencia a la actividad delictiva que implica la compra, venta o intercambio de información confidencial o datos robados sin la autorización del legítimo propietario de esos datos. Estos datos pueden abarcar información personal, financiera, médica, empresarial o cualquier otro tipo de información sensible. Este tipo de actividad criminal en el ámbito informático guarda relación con la apropiación de identidades, el fraude cibernético y otros delitos financieros en línea.

2.2.1.2. Medio informático

Fusco (2020) Un medio informático se refiere a cualquier dispositivo o medio empleado para el almacenamiento, procesamiento, transmisión o visualización de datos e información en formato digital o electrónico. Los medios informáticos juegan un papel fundamental en la era de la tecnología de la información y son esenciales en la gestión y el intercambio de datos.

2.2.1.3. Gobernanza de internet

La gobernanza de Internet se refiere al conjunto de principios, normativas, reglas, procedimientos y acuerdos que rigen la administración, regulación y uso de Internet a nivel global. Internet constituye una red mundial que conecta a millones de personas, organizaciones, gobiernos y empresas en todo el mundo, y su gobernanza es esencial para asegurar su funcionamiento efectivo y equitativo (Ford, 2015, p. 139).

2.2.1.4. Los derechos humanos en línea

Los derechos humanos en línea hacen referencia a los derechos fundamentales que las personas poseen en el entorno digital e Internet. Estos derechos representan una extensión de los derechos humanos tradicionales en el mundo físico y son aplicables

al uso de Internet y las tecnologías digitales. A medida que Internet se ha vuelto una parte integral de la vida de muchas personas, la preservación de los derechos humanos en línea ha adquirido un carácter fundamental.

2.2.1.5. Tipicidad de los delitos informáticos

La tipicidad en el contexto de los delitos informáticos se refiere a la caracterización legal de las actividades delictivas que involucran la utilización de computadoras, sistemas de información, redes y tecnologías de la información. En otras palabras, se trata de definir y clasificar jurídicamente las conductas que se consideran delictivas en el ámbito de la informática y la tecnología. La tipicidad representa un principio fundamental del derecho penal que estipula que un acto solo puede considerarse un delito si está claramente definido como tal en la legislación vigente.

2.2.1.6. Dimensiones

- **Sistemas informáticos** Los sistemas informáticos son conjuntos de componentes interconectados que colaboran para procesar, almacenar, administrar y transmitir datos e información. Estos sistemas desempeñan un papel esencial en una amplia variedad de aplicaciones, desde dispositivos personales como computadoras y teléfonos inteligentes hasta sistemas empresariales y servidores en la nube (Urpeque, 2019, p. 47).
- **Datos informáticos** Los datos informáticos se refieren a la información representada en formato digital o electrónico que es procesada, almacenada y transmitida por sistemas informáticos, como computadoras y dispositivos electrónicos. Estos datos pueden adoptar diversas formas, incluyendo texto, números, imágenes, sonido, video y mucho más (Enciclopedia Etecé, 2023).
- **Acceso ilícito** El acceso ilícito, en el ámbito de la informática y la tecnología, se

refiere a la actividad ilegal que implica obtener acceso no autorizado a sistemas informáticos, redes, cuentas o recursos digitales. Esto implica ingresar o acceder de forma no permitida a sistemas, dispositivos o servicios que generalmente están protegidos mediante contraseñas, medidas de seguridad y autorizaciones (BCN, 2022).

2.2.2. Derecho a la intimidad personal

El derecho a la intimidad personal es un concepto fundamental en el campo de los derechos humanos que garantiza a las personas el control y la privacidad sobre su vida personal y la información relacionada con ella. Este derecho protege a las personas de la intromisión no autorizada en sus asuntos personales, su vida privada y su espacio personal. El derecho a la intimidad personal está reconocido en muchas constituciones y tratados internacionales de derechos humanos, y su alcance puede variar ligeramente según la jurisdicción y las leyes específicas. Según Muñoz (2018).

2.2.2.1. Información íntima

Arellano (2021) La información íntima se refiere a datos personales y privados relacionados con la vida personal, emocional o privada de una persona. Esta información a menudo comprende detalles personales que no se comparten de forma pública y que se consideran altamente sensibles. La protección de esta información es esencial para salvaguardar la dignidad y la autonomía de las personas.

2.2.2.2. Acceso indebido a la plataforma de datos

Mayer (2018) Para prevenir el acceso no autorizado a una plataforma de datos, es fundamental implementar sólidas medidas de seguridad, como el uso de contraseñas seguras, autenticación de dos factores, supervisión de la

actividad de los usuarios y la protección contra amenazas cibernéticas. Además, es crucial educar a los usuarios sobre las mejores prácticas de seguridad en línea para evitar caer en trampas de ingeniería social o divulgar sus credenciales de acceso. En caso de sospecha de acceso no autorizado, se deben tomar medidas para investigar y mitigar la situación, así como informar a las autoridades competentes si es necesario.

2.2.2.3. Violación a la intimidad

Jacobo y Quispe, La violación a la intimidad se refiere a la acción de invadir, acceder o revelar información personal o privada de una persona sin su consentimiento. Esto puede implicar la exposición de detalles íntimos o personales que normalmente se considerarían privados y que están relacionados con la vida personal de alguien. Las violaciones a la intimidad pueden presentarse en diversas formas y contextos, y pueden acarrear graves consecuencias legales y personales.

2.2.2.4. Dimensiones

- Intimidad La intimidad alude a la esfera personal, privada y reservada de la vida de una persona. Incluye áreas y aspectos de la vida que se consideran fuera del alcance del escrutinio público y que están protegidos de la intrusión o divulgación no deseada. La intimidad engloba una amplia gama de contextos y aspectos de la vida de una persona y es esencial para su dignidad, autonomía y bienestar (Palacios, 2021).
- Privacidad La privacidad se refiere al derecho y la capacidad de una persona para mantener y controlar la información personal, actividades y asuntos propios, alejados del escrutinio o acceso no deseado por parte de otros. La privacidad representa un aspecto

fundamental de la dignidad y autonomía de las personas, y se considera un derecho humano fundamental (Palacios, 2021).

- Reserva La reserva puede ser una práctica necesaria en muchos aspectos de la vida, especialmente cuando se trata de proteger la privacidad, mantener la confidencialidad o tomar decisiones estratégicas. Sin embargo, la reserva también puede ser un tema delicado en ciertas situaciones, ya que equilibrar la necesidad de mantener la privacidad con la necesidad de transparencia y comunicación abierta puede ser un desafío. La aplicación de la reserva en un contexto específico depende de las circunstancias y las normas culturales y legales aplicables (Palacios, 2021).

2.3. Bases Filosóficas

Teoría descriptiva La privacidad es un conjunto de derechos fundamentales que se encuentran respaldados por leyes y regulaciones relacionadas con la protección de la privacidad, la seguridad de los datos y otros aspectos legales. No obstante, en determinados contextos, las infracciones de la intimidad pueden resultar en medidas legales o cargos por delitos vinculados con la vulneración de la privacidad.

Las leyes y normativas que salvaguardan la privacidad y la intimidad de las personas varían según la jurisdicción, pero generalmente abordan cuestiones como la protección de datos personales, la interceptación de comunicaciones privadas, la divulgación no autorizada de información confidencial y la seguridad de datos médicos y financieros.

Teoría del delito y su concepción filosófica La teoría del delito es una rama del derecho penal que se enfoca en el análisis de los elementos constitutivos de un delito y los principios esenciales que rigen la responsabilidad penal. Su propósito es comprender

y definir qué constituye un delito y cómo se aplica la responsabilidad penal a las personas que cometen actos delictivos. Además, la teoría del delito suele tener fundamentos filosóficos que se reflejan en su concepción y en sus principios subyacentes, como lo señalan Peña y Almanza (2010).

Para Peña y Almanza (2010). La acción u omisión: Hace referencia a la conducta llevada a cabo por el individuo que podría considerarse como un delito. La culpabilidad: Implica determinar si el individuo actuó con culpabilidad, lo que comúnmente se traduce en la intención de cometer el delito o la negligencia en sus acciones. (Peña y Almanza, 2010, p. 66). La antijuridicidad: Se refiere a la ilegalidad de la conducta, es decir, si la acción u omisión viola la ley. (Peña y Almanza, 2010, p. 68).

La teoría del delito encuentra sus raíces filosóficas en la filosofía del derecho y la ética, abordando cuestiones fundamentales sobre la responsabilidad individual y la justicia (Silva, 1992).

2.4. Definiciones de términos básicos

- Hacking: Se refiere a la acción de ingresar a sistemas informáticos o redes sin la debida autorización con la intención de sustraer información, causar daño o llevar a cabo actividades ilícitas.
- Phishing: Una estrategia que implica engañar a individuos para que divulguen información personal o confidencial, como contraseñas o datos financieros, generalmente mediante el uso de correos electrónicos o sitios web falsificados.
- Malware: Programas informáticos maliciosos desarrollados con la finalidad de perjudicar o acceder de manera no autorizada a sistemas informáticos. Esta categoría abarca virus, gusanos, troyanos y ransomware.

- Ransomware: Una variedad de malware que cifra los archivos de una víctima y demanda un rescate para descifrarlos. Si el rescate no se abona, los archivos pueden quedar inaccesibles.
- Ataque de denegación de servicio (DoS): Un ataque que satura un sistema o página web con tráfico dañino con el fin de hacerlo inaccesible para usuarios legítimos.
- DoS distribuido (DDoS): Una versión del ataque de denegación de servicio en la que se emplea una red de dispositivos comprometidos para ejecutar la ofensiva.
- Ingeniería social: La estrategia de manipular a personas para obtener datos confidenciales o acceso a sistemas informáticos, generalmente mediante la persuasión o la manipulación psicológica.

2.5. Hipótesis de investigación

2.5.1. Hipótesis general

Los delitos informáticos contra los datos influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023.

2.6. Operacionalización de las variables

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumento
Delitos informáticos	Los delitos informáticos, también conocidos como cibercrimes, son actividades ilegales que se llevan a cabo mediante el uso de computadoras, redes de computadoras y tecnología de la información. Estos delitos involucran violaciones de la seguridad cibernética y pueden variar en gravedad y alcance. (Ruiz, 2016)	Se considera la medición de la variable teniendo en consideración las tres dimensiones: Sistemas informáticos, datos informáticos y acceso ilícito, que involucran como indicadores a los datos personales, al uso de componentes electrónicos, características de almacenamiento de datos y seguridad del sistema de información.	Sistemas informáticos Datos informáticos Acceso ilícito	<ul style="list-style-type: none"> • Datos personales • Uso de software • Uso de hardware • Almacenamientos • Procedimientos • Aplicaciones • Vulneración • Intromisión • Extracción 	Cuestionario y Guía de entrevista de delitos informáticos
Derecho a la intimidad personal	El derecho a la intimidad personal es un derecho fundamental que protege la esfera privada de las personas y su capacidad de mantener información personal y actividades fuera del escrutinio público sin su consentimiento. Este derecho reconoce la importancia de la autonomía, la dignidad y la privacidad de los individuos.. (Muñoz, 2018)	Se considera la medición de la variable teniendo en consideración las tres dimensiones: Intimidad, privacidad y reserva, que involucran los indicadores de vulneración, resarcimiento, afectación, formulación, regulación, limitación, capacidad de personal y indemnización.	Intimidad Privacidad Reserva	<ul style="list-style-type: none"> • Vulnerar • Resarcir • Afectar • Atentar • Formular • Limitar • Alteración • Capacidad • Indemnizar 	Cuestionario y Guía de entrevista de Derecho a la intimidad personal

CAPÍTULO III

METODOLOGÍA

3.1. Diseño de la investigación

3.1.1. Tipo de investigación

Dado el contexto y los objetivos planteados, la investigación que se llevó a cabo en este estudio se enfocó en un enfoque cuantitativo. De acuerdo con la definición de Chenet (2018), la investigación aplicada se orienta principalmente hacia la resolución de problemas prácticos, y aunque la generación de conocimiento teórico es un objetivo secundario en este caso. Además, esta investigación se llevará a cabo en un período de tiempo específico, lo que la caracteriza como de tipo transversal, ya que se recopilarán datos en un momento determinado.

3.1.2. Nivel de investigación

El enfoque de la investigación se consideró descriptivo, basándose en los principios de Bernal (2012), que se centra en la relación entre las variables de estudio y busca identificar los elementos comunes, independientemente de su grado de relevancia.

3.1.3. Diseño de investigación

La investigación se clasificó como no experimental en términos de diseño, siguiendo la definición de Hernández, Fernández y Baptista (2014). Esto significa que se llevó a cabo mediante la observación de las dos variables de estudio en su entorno natural, sin ninguna manipulación deliberada. Esto permitió el análisis y la descripción de las variables en un momento específico.

3.2. Población y muestra

3.2.1. Población

El grupo de personas objeto de estudio estaba compuesto por un total de 60 individuos, que incluía tanto a operadores de justicia como a víctimas o afectados en relación con la violación de su intimidad personal en la provincia de Barranca durante el año 2023.

3.2.2. Muestra

La muestra de estudio lo conformada por 28 personas, entre operadores de justicia y víctimas o agraviados al derecho a su intimidad personal en la provincia de Barranca en el año 2023; sustentada en el modelo estadístico de muestra finita:

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

Donde:

N: tamaño de la población.

Z: Grado de confianza que se establece.

E: Error absoluto precisión de la estimación de la proporción.

P: Proporción de unidades que poseen el atributo de interés.

Q: la diferencia aritmética de P respecto a la unidad.

Entonces reemplazando tenemos:

$$n = \frac{(1.96)^2(0.5)(0.5)(60)}{(0.05)^2(59) + (1.96)^2(0.5)(0.5)} = 52 \text{ personas}$$

Tamaño final de muestra (n) corregida por KISH:

$$n = \frac{n_0}{1 + \frac{n_0}{N}}$$

Entonces reemplazando tenemos:

$$n = \frac{52}{1 + \frac{52}{60}} = 28 \text{ personas}$$

Personas	Muestra
Fiscales	2
Abogados litigantes	4
Víctimas o agraviados	22

Criterios de inclusión

- 1) Operadores de justicia que laboran en la provincia de Barranca.
- 2) Víctimas o agraviados del derecho a la intimidad personal en la provincia de Barranca.
- 3) Operadores de justicia y víctimas o agraviados que deseen colaborar con la investigación voluntariamente.

Criterios de exclusión

- 1) Operadores de justicia que no laboran en la provincia de Barranca.
- 2) Víctimas o agraviados del derecho a la intimidad personal fuera de la provincia de Barranca.
- 3) Operadores de justicia y víctimas o agraviados que no desean colaborar con la investigación.

Criterios éticos

- 1) Respeto: El principio del respeto para la información brindada por las personas que intervienen en la investigación.
- 2) Beneficio: El principio de beneficencia, porque el desarrollo de la investigación no afectara de manera negativa las costumbres o su identidad cultural de las personas, por lo contrario, esto generara nuevos conocimientos.
- 3) Justicia: El principio de justicia, para lo cual buscara brindar seguridad y confiabilidad de la información de las personas que intervienen en la investigación.

3.3. Técnicas de recolección de datos

3.3.1. Técnicas

En esta tesis se utilizaron tanto encuestas como entrevistas como técnicas de investigación, ya que son herramientas comunes en trabajos científicos y proporcionan una visión más completa de la población en estudio. Siguiendo la sugerencia de Hernández y colaboradores (2014), una de las ventajas principales de estas técnicas radicó en su eficiencia en términos de tiempo y recursos humanos, ya que pudimos aplicarlas directamente al grupo de interés. Además, es importante destacar que el proceso general de análisis de la información recopilada a través de estas técnicas se describe en la sección de instrumentos, donde se detalla el uso del cuestionario estructurado como método específico en este caso.

3.3.2. Instrumentos

Se utilizaron dos instrumentos en esta investigación: un cuestionario y una guía de entrevista. En este estudio, se presentó un cuestionario con 12 preguntas y

una guía de entrevista con 12 preguntas. Estos instrumentos emplearon la escala de Likert y respuestas abiertas, respectivamente (consulte el Anexo 2).

El cuestionario y la guía de entrevista formaron la base para la presentación del informe de esta investigación. El objetivo específico de estos instrumentos era investigar la relación entre las dos variables de interés, con la intención de proporcionar información valiosa que beneficie tanto a las instituciones judiciales en relación con los delitos informáticos como a la protección del derecho a la intimidad personal.

Validación

Instrumento de delitos informáticos: Estuvo conformada por tres dimensiones, las cuáles son: Sistemas de informáticos, datos informáticos y acceso ilícito; las cuales se midieron esta información con 5 ítems (Ver Anexo 3).

Instrumento de derecho a la intimidad personal: Está conformada por tres dimensiones, las cuáles son: Intimidad, privacidad y reserva; las cuales se midieron esta información con 5 ítems (Ver Anexo 3).

Guía de entrevista: La estructura de esta guía de entrevista con 12 ítems.

Confiabilidad

La evaluación de la confiabilidad se llevará a cabo mediante el coeficiente Alfa de Cronbach, el cual se aplicará a cada uno de los instrumentos de investigación. La ventaja clave de este coeficiente radica en que solo requiere una única administración del instrumento de medición. Este coeficiente puede variar en un

rango de 0 a 1, donde un valor de 0 indica una confiabilidad nula, mientras que un valor de 1 representa una confiabilidad total.

En la siguiente tabla se muestran los coeficientes calculados para cada dimensión del test utilizando la siguiente fórmula:

$$\alpha = \frac{K}{1+(K-1) \cdot \frac{\sum s_i^2}{s_T^2}}$$

Donde:

- K es el número de ítems.
- $\sum S_i^2$ es la suma de la varianza de cada ítem.
- $\sum S_T^2$ es la varianza total de las filas.

3.4. Técnicas para el procesamiento de la información

En cuanto al muestreo, se optó por la técnica de muestreo aleatorio simple, ya que se seleccionaron al azar los residentes dentro del ámbito provincial.

Respecto a la recopilación de datos, se llevaron a cabo los siguientes pasos:

- Adquisición de información por parte del investigador.
- Organización de la información recopilada.
- Clasificación de los datos en categorías relevantes.
- Elaboración de una tabla de especificaciones que detallaba los datos esenciales.
- Implementación de la encuesta entre los participantes.
- Creación de cuadros estadísticos para resumir los resultados.
- Realización de pruebas de entrada, proceso y salida para verificar la calidad de los datos.

La información recabada se ingresó en una base de datos mediante el software SPSS 26.0. Este enfoque facilitó la presentación ordenada de los datos en forma de tablas y gráficos, lo que simplificó el análisis y la interpretación posteriores. Además, se recurrió a la estadística inferencial, específicamente basada en la distribución normal, para fundamentar la evaluación de hipótesis en el estudio.

3.5. Matriz de consistencia

La representación explícita se verá en el Anexo 1.

CAPÍTULO IV

RESULTADOS

4.1. Análisis de resultados

4.1.1. Resultados del cuestionario

Tabla 1

Categoría de los delitos informáticos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido Deficiente	1	4,5	4,5	4,5
Regular	5	22,7	22,7	27,3
Bueno	16	72,7	72,7	100,0
Total	22	100,0	100,0	

Nota: Elaboración propia

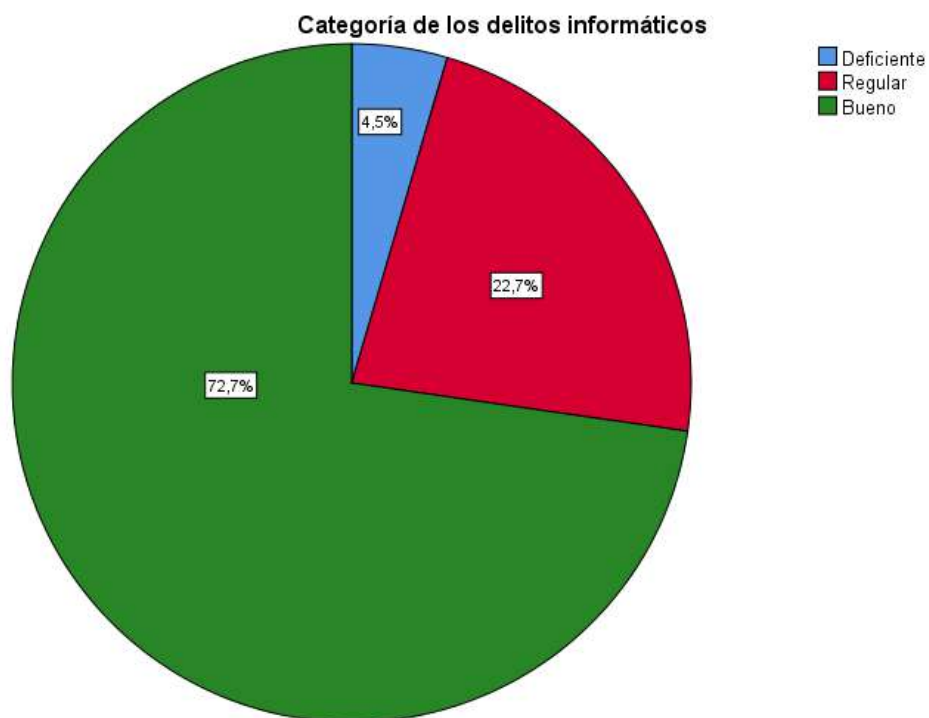


Figura 1. Categoría de los delitos informáticos

A partir de los resultados presentados, se puede destacar que se obtuvieron como resultado de la aplicación de un cuestionario sobre delitos informáticos, el cual se dividió en tres opciones. Se observa que:

- Un 4,5% de los encuestados indican que siguen procedimientos que promueven la prevención de delitos informáticos, lo que los coloca en la categoría de rendimiento deficiente en la provincia de Barranca.
- Un 22,7% de los encuestados manifiestan que siguen procedimientos para prevenir delitos informáticos, lo que los califica en la categoría de rendimiento regular.
- El 72,7% de los encuestados señalan que siguen procedimientos que promueven la prevención de delitos informáticos, y esto los ubica en la categoría de rendimiento bueno. Esto significa que estos individuos no publican información privada en sus redes sociales, son cautelosos en sus publicaciones en entornos digitales, no comparten imágenes ni datos informáticos con otros miembros de su entorno social, evitan involucrarse en conflictos sociales y cumplen con las leyes establecidas en la legislación vigente.

En resumen, la mayoría de los encuestados demuestran prácticas seguras y responsables en línea, lo que se refleja en la protección de su privacidad y el cumplimiento de las normativas legales vigentes.

Tabla 2

Categoría del derecho a la intimidad personal

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Bajo	0	0,0	0,0	0,0
Medio	5	22,7	22,7	22,7
Alto	17	77,3	77,3	100,0
Total	22	100,0	100,0	

Nota: Elaboración propia

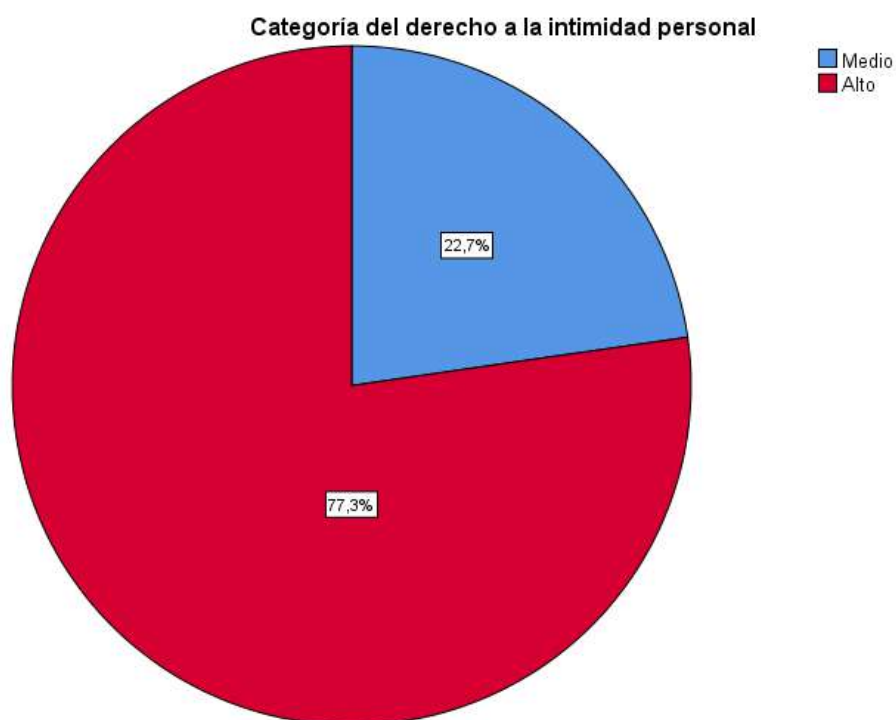


Figura 2. Categoría del derecho a la intimidad personal

Basándonos en los resultados presentados, se puede observar que se derivan de la aplicación de un cuestionario relacionado con el derecho a la intimidad personal. Estos resultados se categorizaron en tres opciones:

Ningún encuestado considera que la vulneración del derecho a la intimidad personal sea de categoría baja en la provincia de Barranca.

El 22,7% de los encuestados opina que la vulneración del derecho a la intimidad personal se encuentra en la categoría media.

El 77,3% de los encuestados considera que la vulneración del derecho a la intimidad personal se sitúa en la categoría alta.

En otras palabras, la mayoría de los encuestados está consciente de que la vulneración de la intimidad personal debe ser sancionada de manera ejemplar y

abogan por el aumento de las penas para aquellos que infringen este derecho. También sugieren modificar las normativas legales, como el código civil y penal, para lograr mejores resultados en la protección de la intimidad personal. Asimismo, expresan la necesidad de supervisar los medios de comunicación, tanto impresos como digitales, ya que pueden poner en peligro este derecho. Además, se reconoce que las personas influyentes en las redes sociales tienen una mayor probabilidad de ser víctimas de la vulneración de su intimidad, y se destaca que cualquier vulneración de la intimidad de una persona también afecta a su entorno familiar.

4.1.2. Resultados de la guía de entrevistas

Tabla 3

Listas de especialistas

Especialista	Nombres y Apellidos	Cargo
1	Ramu Raymundo Suarez	Fiscal
2	Luis Navarro Martínez	fiscal
3	Fersey Mathus Bustamante Aguilar	Abogado
4	Berenice Carolina Flores Carrillo	Abogado
5	Héctor Steven Olortegui Mendoza	Abogado
6	José Vergara Vásquez	Abogado

Nota: Elaboración propia

Objetivo general: “*Determinar la influencia de los delitos informáticos contra los datos sobre la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023*”.

Pregunta 1: ¿De qué forma los delitos informáticos contra los datos vulneran el derecho a la intimidad personal?

Tabla 4

Pregunta 1

Especialista	Opinión
1	Es varia las formas en las que vulneran el derecho a la intimidad, pero aún más con el uso de los elementos tecnológicos como el celular. Los archivos que contienen datos personales, en muchas ocasiones llegan a manos de inescrupulosos que lo utilizan ya sea para el chantaje o para la venta de esas escenas (en personales públicos).
2	Los datos que la persona provee por medio de la red, son datos tan personales como puede ser nuestro Documento de Identidad Nacional, y ello requiere que la información sea estrictamente secreta, entra la persona y la entidad a la cual se le menciona dicha información. Los delitos que atentan contra dicha confidencialidad o por acción ajena, permiten que dichos datos puedan ser utilizados o modificados, es una amenaza potencial a la intimidad de la persona, debido a que la información puede ser utilizada para distintos fines maliciosos.
3	Los delitos informáticos vulneran el derecho a la intimidad personal porque afectan a la privacidad y reserva de los derechos de información contenidas en archivos virtuales, ya sea redes sociales, correos electrónicos entre otros. Por lo cual los operadores jurídicos del Estado deben brindar la protección debida.
4	Afectan al derecho a la intimidad, privacidad y reserva de la información contenida en estos, por lo tanto, los operadores del derecho deben tener presente la protección del objeto material (información) contemplado en el uso de las tecnológicas de la información.
5	Son varias las formas, con el uso de un computador, celulares, entre otros, los mismos que son utilizados para estafas chantajes, extorsiones.
6	Personal, íntima, ya que muchos casos se publican en la internet e en medios digitales, sin accesos ni restricciones.

Nota: Elaboración propia

Pregunta 2: ¿Cuáles son las consecuencias que conlleva los delitos informáticos en la vulneración del derecho a la intimidad personal?

Tabla 5

Pregunta 2

Especialista	Opinión
1	Son muchas, pero resaltaría la desconfianza en el archivamiento de datos íntimos en los sistemas informáticos.
2	Pueden ser varias las consecuencias que trae los delitos informáticos, enfatizando a los que atentan contra la intimidad personal, tenemos: a) El robo de identidad: Se comprometen los datos personales, para suplantar la identidad de otra persona. Generalmente se emplea para delitos de estafa. b) Violación a la privacidad de las redes sociales: Consiste en la invasión de la privacidad, donde los delincuentes logran acceder a las redes sociales de sus víctimas. Ello puede llevar a la divulgación de información personal o íntima. c) El ciberacoso y/o acecho en línea: Mediante esta modalidad, los delincuentes acosan, amenazan, intimidan u hostigan a sus víctimas, pudiendo incluso espiarlos y saber su ubicación exacta.
3	Las consecuencias que conlleva los delitos informáticos es la vulneración de derecho a la intimidad personal es de prisión preventiva de la libertad, así como pagos de multas por un periodo determinado.
4	Sera castigado con una pena de prisión de tres meses a un año o multa de seis meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros, imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar.
5	Generan diversas consecuencias, siendo una de ellas la privación del derecho a la libertad.
6	La lesividad de los derechos fundamentales.

Nota: Elaboración propia

Pregunta 3: ¿Se aplican adecuadamente las sanciones penales en coherencia al accionar de este tipo de delito informático, las cuales atentan al derecho a la intimidad personal?

Tabla 6

Pregunta 3

Especialista	Opinión
1	Desconozco sobre ello, dado a que en Lima ya se vienen implementando fiscalías especializadas en delitos informáticos.
2	Generalmente no se visualiza una accionar sancionador por parte de las autoridades, sino más bien la ejecución de acciones preventivas promovidas por los mismos. Como puede ser el caso de: “advertir que el uso de la clave de seguridad de tu cuenta bancaria, es sumamente personal y no debes compartirla con nadie.”
3	No, sabemos que en el Perú las sanciones penales para este tipo de delitos son bajas y existen pocos casos que se hayan aplicado la máxima pena.
4	No, en nuestro país recién se viene tomando en consideración estos tipos de delitos, por lo cual no se vienen aplicando las sanciones de forma adecuada.
5	En nuestra Provincia de Barranca, no se vienen aplicando estos tipos de delito, siendo que en la ciudad de lima ya se viene teniendo caso.
6	No, ya que son difíciles de detectar.

Nota: Elaboración propia

Objetivo específico 1: “*Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la intimidad personal en la provincia de Barranca en el año 2023*”.

Pregunta 4: ¿Los Delitos Informáticos, se han convertido en una nueva forma de atentar y vulnerar la intimidad de las personas a través del uso de la tecnología en la provincia de Barranca?

Tabla 7

Pregunta 4

Especialista	Opinión
1	No existen casos palpables, ya que se ven como otros delitos como trata de personas, explotación sexual, etc.
2	Hemos podido evidenciar que conforme va avanzando la tecnología, los delitos también evolucionan con ello. Hace 100 años atrás era una ficción hablar de delitos informáticos, pero hoy podemos apreciar que es una realidad y un peligro latente para la provincia de Barranca. La forma en la que los delincuentes buscan obtener nuestra información, generalmente se da por medio de encuestas, sorteos o llamadas de “oportunidad laboral”, medios por los cuales disfrazan su fechoría con cuentos para concretar su delito. En conclusión, puedo afirmar que sí, los delitos informáticos tienden a vulnerar mucho la intimidad de la persona.
3	Así es, los delitos informáticos, se han convertido en una nueva forma de atentar y vulnera la intimidad de las personas a través del uso de la tecnología, ya que ahora toda persona tiene al alcance un aparato celular en la que permite identificar a través de las redes sociales a su víctima.
4	Si, en estos nuevos tiempos la tecnología se ha convertido en una herramienta mortal para la intimidad de las personas, siendo que en nuestra provincia de barranca los más vulnerables son los jóvenes y profesionales.
5	En nuestra Provincia de Barranca aún no se ven casos denunciados por estos delitos.
6	Si, ya que aprovechan las plataformas digitales para cometer este tipo de delito.

Nota: Elaboración propia

Pregunta 5: ¿Cómo el derecho a la intimidad personal garantiza el resarcimiento del daño?

Tabla 8

Pregunta 5

Especialista	Opinión
1	Sólo en casos penales con sentencia y con reparación civil. Se entiende que la intimidad personal es un derecho fundamental establecido en nuestra Constitución, y su vulneración genera en la persona un daño profundo, pues es exponer a público abierto toda su vida íntima, vida en la cual la sociedad no debe participar y mucho menos conocer. El derecho a la intimidad personal, nos permite hacer frente a estas vulneraciones, por medio de medidas compensatorias, tales como: a) La indemnización económica b) Las acciones legales contra los responsables c) La reparación moral (disculpas públicas)
2	Cuando se da cumplimiento a la norma legal aplicable, puede ser en materia penal o civil.
3	Se prevé el derecho de toda persona a ser protegida respecto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, así como a ataques ilegales a su honra y reputación.
4	Por la correcta aplicación de las normas.
5	Muchas veces el daño no se repara, debido a nuestro sistema penal garantista.
6	

Nota: Elaboración propia

Pregunta 6: ¿Considera que este tipo de delitos a nivel tecnológico afecta psicológicamente a la víctima?

Tabla 9

Pregunta 6

Especialista	Opinión
1	Si Considero que sí, ya que la víctima tiende a padecer de mucho estrés, a consecuencia del delito. A ello puede sumársele problemas de ansiedad y depresión
2	Si afecta considerablemente, ya que las personas afectadas muchas veces comienzan a tener estados de ansiedad, angustia entre otros.
3	

- 4 Si, y considero que aumenta estados de ansiedad, angustia y desanimo, con lo cual nos hace más difícil aprender a entender y gestionar esas emociones.
- 5 Si
- 6 Pornografía infantil, extorsión y acoso.

Nota: Elaboración propia

Objetivo específico 2: “*Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la privacidad personal en la provincia de Barranca en el año 2023*”.

Pregunta 7: ¿Consideraría usted que los delitos informáticos de datos, atenta contra la privacidad personal de los ciudadanos de la provincia de Barranca, mediante el uso de la tecnología?

Tabla 10
Pregunta 7

Especialista	Opinión
1	Si Sí, principalmente porque los delincuentes informáticos tienden a usar mucho de la tecnología para cometer sus actos delictivos, como puede ser: chips de línea móvil duplicadas, el uso de softwares para robar información, los mensajes de texto con redireccionamiento a paginas “fakes” sumamente detalladas o similares a alguna entidad bancaria, etc. De tal manera que los delincuentes aprovechan mucho de la tecnología para acceder a los datos personales de los ciudadanos.
2	Si Por supuesto, vulnera claramente el derecho a la intimidad a las personas, lo cual genera una lesividad a los derechos fundamentales de la persona en nuestra provincia de Barranca.
3	Si Si, incluso con falsos perfiles para insultar.
4	Si
5	Si, incluso con falsos perfiles para insultar.
6	

Nota: Elaboración propia

Pregunta 8: ¿Es necesario la formulación de medidas o acciones de nivel tecnológico para frenar este tipo de delitos informáticos según los avances tecnológicos?

Tabla 11

Pregunta 8

Especialista	Opinión
1	Considero que sí. Deben ir en forma paralela
2	Opino que sí, debido a que conforme vaya avanzando la tecnología, los delitos informáticos se irán incrementando y agravando; y es necesario salvaguardar la seguridad informática de los ciudadanos, más allá de una simple advertencia. Un gran paso que se ha logrado, es el uso de autenticadores, pero ello no siempre garantiza la seguridad informática.
3	Si, ya que nos va a permitir la agilidad de las investigaciones.
4	Así es, el usuario debe prevenir y realizar diversas acciones: cambiar contraseña de sus correos electrónicos/redes sociales ni dejar abierta los mismos, actualizar los antivirus, no usar redes públicas para transacciones.
5	Si, nos ayudarían muchísimo a la agilización de los procesos de investigación
6	Si, mediante el uso de medios informáticos y tecnológicos.

Nota: Elaboración propia

Pregunta 9: ¿Consideraría usted que existen límites en el desarrollo de un delito informático hacia la privacidad personal en la provincia de Barranca?

Tabla 12
Pregunta 9

Especialista	Opinión
1	No Hoy en día, los delincuentes tienen a la mano distintas herramientas para poder cometer sus fechorías, tienen todas las facilidades para cometer delitos informáticos, un claro ejemplo de ello son las páginas web falsas, detalladas
2	hasta con el más mínimo detalle, en el cuál envían mensajes a los usuarios para engatusarlos a fin de que proporcionen sus datos. En definitiva, opino que no existen límites para que el delito informático se vea imposibilitado de cometerse.
3	No, por la inaplicación de las normas.
4	Si, la preparación de los efectivos policiales y fiscales, son deficientes lo que hace que el trabajo de investigación sea muy débil.
5	Si, por que no se están aplicando correctamente la normatividad.
6	No, no existe, al contrario buscan atentar más la intimidad de la persona.

Nota: Elaboración propia

Objetivo específico 3: “*Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la reserva personal en la provincia de Barranca en el año 2023*”.

Pregunta 10: ¿Los delitos informáticos pueden ocasionar una alteración o una usurpación en los datos de las víctimas, a través de las redes sociales en la provincia de Barranca?

Tabla 13

Pregunta 10

Especialista	Opinión
1	Si
2	Efectivamente, como se ha comentado con anterioridad, las redes sociales vienen a ser el punto perfecto para los delincuentes para cometer los delitos informáticos, debido a que dichas redes permiten disfrazar u ocultar la identidad del delincuente, y con ello ganar más confianza con la víctima para que brinde sus datos personales. Una vez obtenido los datos de su víctima, este tiene control y libertad de realizar cualquier acto que le favorezca.
3	Si
4	Si, tienen gran repercusión en la criminalidad económica actual porque colisionan con una economía globalizada y que emplea sistemas financieros, operaciones comerciales, transacciones bancarias virtuales, así como sistemas informáticos.
5	Si
6	Si, por ejemplo en la suplantación de identidad a través de falsos perfiles.

Nota: Elaboración propia

Pregunta 11: ¿Incrementar la capacitación o actualizar a los operadores del derecho, en la defensa de las víctimas de este tipo de delitos informáticos, generara una efectividad de las sanciones en la provincia de Barranca?

Tabla 14

Pregunta 11

Especialista	Opinión
1	Si
2	En mi opinión, considero que sí, podría haber una leve mejoría, pero los resultados no serían inmediatos.
3	Si
4	Así es, sabemos que este tipo de delito ya tiene un buen tiempo operándose, sin embargo, las tipificaciones son recientes y muchas de ellas no son efectivas, por lo cual es necesario realizar capacitaciones respecto a este tema.

5	Si
6	Si para tener un proceso que garantice el debido proceso y obtener justicia.

Nota: Elaboración propia

Pregunta 12: ¿Consideraría usted que los medios informáticos son un daño indemnizable?

Tabla 15

Pregunta 12

Especialista	Opinión
1	Si
2	Sí, porque se está atentando directamente contra la vida personal del individuo, y ello, al igual que el honor, son daños que permanecerán en el tiempo, por más que se compense, la vulneración queda plasmada tanto en la sociedad como en la propia persona.
3	Si
4	Sí, porque si el delito ya está materializado, se deben resarcir los daños generados.
5	Si
6	Sí, porque contiene todos los requisitos que establece la ley para ser indemnizados.

Nota: Elaboración propia

4.2. Contrastación de hipótesis

Prueba de normalidad de la variable delitos informáticos

H₀: Los datos de la variable delitos informáticos cultural no difieren de una distribución normal

H₁: Los datos de la variable delitos informáticos difieren de una distribución normal

Nivel de significancia $\alpha = 5\%$ o $\alpha = 0.05$

Se empleará el estadístico de prueba de Shapiro-Wilk; porque el tamaño es menor o igual a 50.

Tabla 16

Prueba de Normalidad de delitos informáticos

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Delitos informáticos	,921	22	,080

a. Corrección de significación de Lilliefors

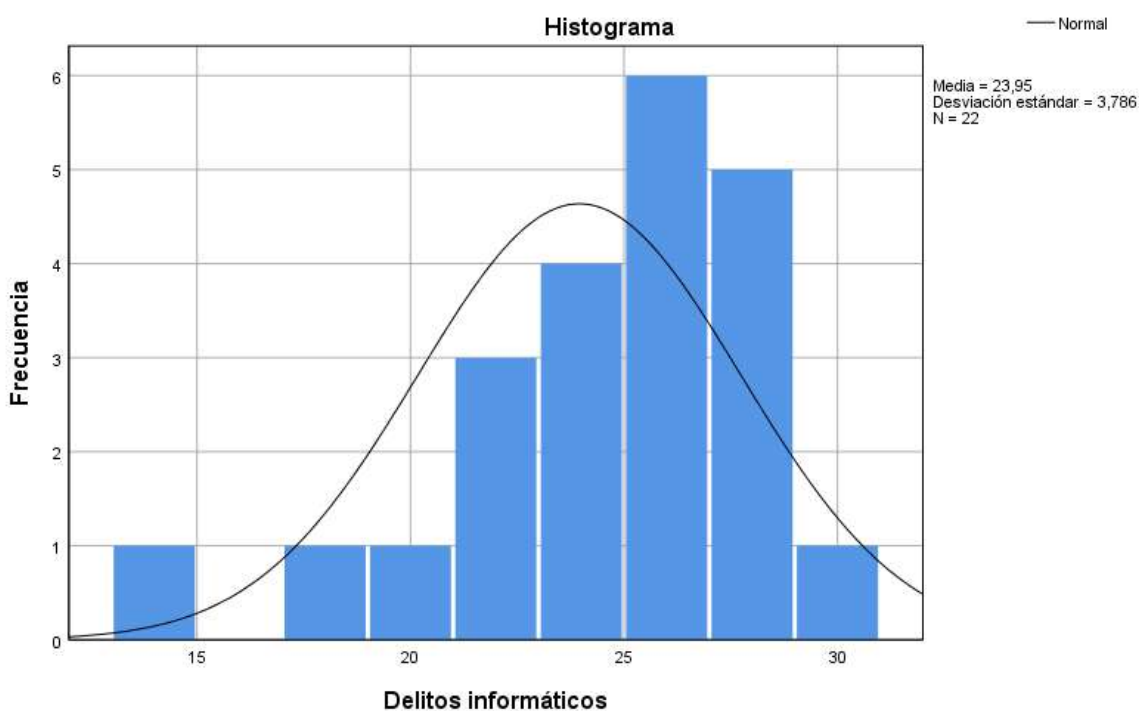


Figura 3. Histograma y curva normal de delitos informáticos

Si p –valor (Sig.) > 0.05; se acepta la hipótesis nula

Conclusión

Como el p-valor (Sig.) = 0.000 como este valor es mayor a 0,05 se infiere que hay suficiente evidencia estadística para aceptar la hipótesis nula, concluyendo que las puntuaciones de la variable delitosinformaticos presentan una distribución normal.

Prueba de normalidad de la variable derecho a la intimidad personal

H₀: Los datos de la variable derecho a la intimidad personal no difieren de una distribución normal

H₁: Los datos de la variable derecho a la intimidad personal difieren de una distribución normal

Nivel de significancia $\alpha = 5\%$ o $\alpha = 0.05$

Se empleará el estadístico de prueba de Shapiro-Wilk; porque el tamaño es menor o igual a 50.

Tabla 17

Prueba de Normalidad de derecho a la intimidad personal

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Derecho a la intimidad personal	,889	22	,018

a. Corrección de significación de Lilliefors

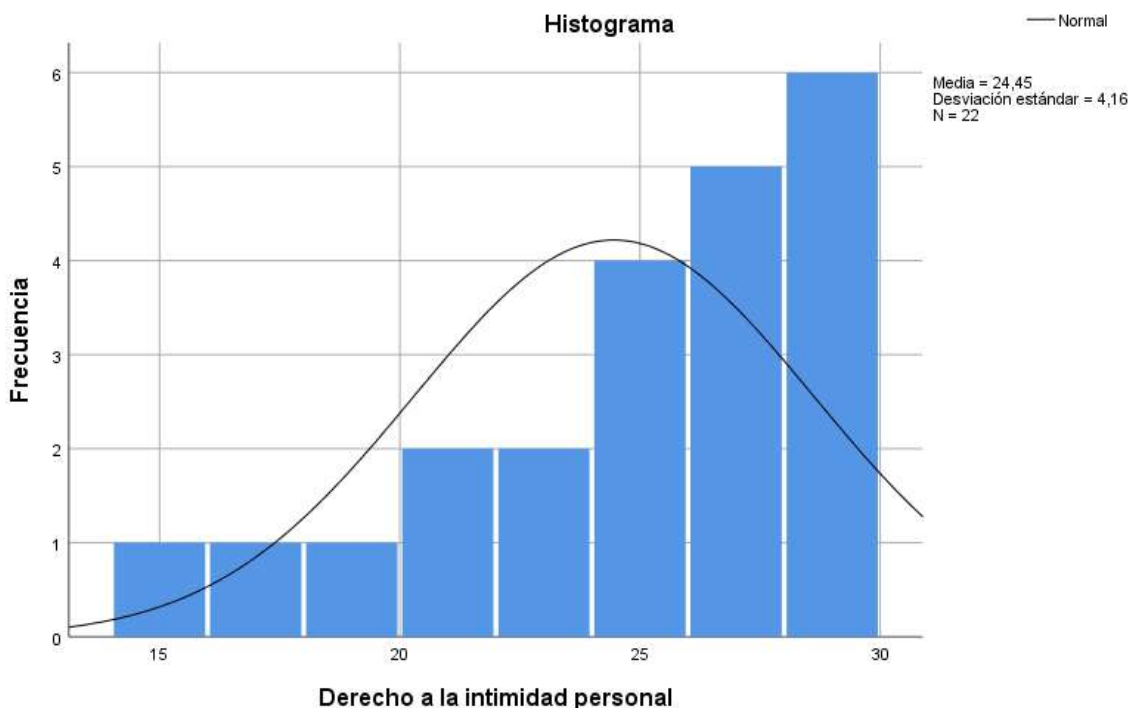


Figura 4. Histograma y curva normal de derecho a la intimidad personal

Si p -valor (Sig.) < 0.05 ; se rechaza la hipótesis nula

Conclusión

Como el p -valor (Sig.) = 0.000 como este valor es menor a 0,05 se infiere que hay suficiente evidencia estadística para rechazar la hipótesis nula, concluyendo que las puntuaciones de la variable derecho a la intimidad personal no presentan una distribución normal.

Hipótesis general

H₀: Los delitos informáticos contra los datos no influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023.

H₁: Los delitos informáticos contra los datos influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023.

Tabla 18

Correlación entre los delitos informáticos (DI) y Derecho a la intimidad personal (DIP)

		DI	DIP
Delitos informáticos	Correlación de Pearson	1	,769**
	Sig. (bilateral)		,000
	N	22	22
Derecho a la intimidad personal	Correlación de Pearson	,769**	1
	Sig. (bilateral)	,000	
	N	22	22

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

Conclusión

Como la sig. (Bilateral)= p-valor =0.000 es menor que la significación $\alpha= 0,05$, se rechaza la hipótesis nula y se acepta la hipótesis alterna. Es decir: “Los delitos informáticos contra los datos influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023”. El valor del coeficiente de correlación de Pearson = 0.769 nos indica estadísticamente que existe una correlación positiva alta; tomado de Bisquerra (2009).

CAPÍTULO V

DISCUSIÓN

5.1. Discusión de resultados

Los resultados presentados en este estudio indican que se ha examinado la influencia de los delitos informáticos en la vulneración del derecho a la intimidad personal en la provincia de Barranca durante el año 2023. Se ha observado una correlación de Pearson de 0.769, lo que representa una correlación positiva alta.

En lo que respecta a la variable de delitos informáticos, se ha identificado que el 4.5% de los encuestados siguen prácticas deficientes en la prevención de estos delitos informáticos, el 22.7% sigue prácticas regulares y el 72.7% sigue prácticas buenas. Esto se traduce en un cuidado por parte de los encuestados en lo que respecta a la divulgación de información privada en sus redes sociales, su comportamiento cauteloso en publicaciones en medios digitales, la reticencia en compartir imágenes o datos informáticos con otros miembros de su entorno social y el cumplimiento de las leyes establecidas en la legislación.

Con relación a la variable del derecho a la intimidad personal, el 22.7% de los encuestados considera que la vulneración de este derecho se sitúa en la categoría media, mientras que el 77.3% opina que se ubica en la categoría alta. Esto sugiere que los encuestados valoran la vulneración de la intimidad de las personas y abogan por sanciones ejemplares, el aumento de las penas para quienes violan este derecho, la modificación de las normativas legales, como el código civil y penal, para obtener mejores resultados, y el control de los medios de comunicación escrita y digital, ya que ponen en riesgo el derecho a la intimidad. También reconocen que las personas influyentes en las redes sociales tienen una mayor probabilidad de ser víctimas de

vulneración de su intimidad, y que cualquier vulneración de la intimidad de una persona también afecta a su entorno familiar.

Resultados similares a estos se han encontrado en otros estudios, como el de Salvador (2022), que destaca cómo la suplantación de identidad, la falsificación y el uso de documentos falsos, la apropiación fraudulenta por medios electrónicos y el acceso no consentido a sistemas informáticos afectan negativamente el patrimonio de las víctimas. Asimismo, el estudio de Zarate (2023) señala la necesidad de leyes más sólidas y protocolos más claros para penalizar a quienes violan la privacidad mediante el uso inapropiado de las redes sociales. Palacios (2021) también aboga por un estudio más profundo y una aplicación adecuada de la naturaleza e imputabilidad de los delitos informáticos contra datos y sus efectos sobre los derechos fundamentales de las personas, destacando que este tipo de delitos tiene una naturaleza autónoma en el Código Penal.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Los resultados obtenidos en el análisis de la hipótesis general revelan una significancia asintótica (valor p calculado = 0.000), que es menor que el nivel de significancia ($p = 0.05$). Por lo tanto, existe suficiente evidencia estadística para rechazar la hipótesis nula y respaldar la hipótesis alternativa que afirma que los delitos informáticos contra los datos ejercen influencia en la vulneración del derecho a la intimidad personal en la provincia de Barranca en el año 2023. Además, se observa una correlación de Pearson de 0.769, lo que se considera una correlación positiva alta según la escala de Bisquerra.
- Se examinó de qué manera el tráfico ilegal de datos afecta la información íntima de las personas, lo que a su vez resulta en la vulneración de la intimidad de las personas en la provincia de Barranca y el surgimiento del tráfico ilegal de datos. Este análisis se enmarca en el contexto del derecho a la intimidad personal, que es un derecho fundamental establecido en la Constitución Política del Perú, en su inciso numeral cuatro.
- Se investigó cómo el medio informático actúa como una herramienta tecnológica que permite el acceso indebido a plataformas de datos. Esto facilita que individuos con intenciones cibernéticas ingresen a la información de las personas en la provincia de Barranca. A través de los argumentos expuestos y con base en la literatura de diversos autores, se pudo confirmar la existencia de delitos

informáticos que vulneran la intimidad de las personas en situaciones de sabotaje o apropiación indebida de información a la que no deberían tener acceso.

6.2. Recomendaciones

- Se recomienda que los expertos en el campo del derecho penal presten especial atención a los derechos fundamentales involucrados en los delitos informáticos. Esto garantizará que los usuarios utilicen información precisa y adecuada a través de medios informáticos, lo que contribuirá a la protección del bien jurídico y reducirá la incidencia de delitos informáticos.
- Se sugiere que los operadores de servicios móviles, a través de los cuales se transmiten los datos personales, implementen rigurosas medidas de seguridad para proteger la información de los usuarios contra posibles delitos que puedan surgir debido a vulnerabilidades. Asimismo, se insta a los profesionales del área de informática a detectar de manera oportuna los cibercrímenes que podrían afectar la privacidad de los usuarios. Además, se les anima a impartir formación sobre cómo proteger la información personal, lo que ayudará a prevenir futuros riesgos.
- Es importante desarrollar plataformas digitales que incorporen validación en tiempo real para prevenir la suplantación de identidad, ya que esta acción permite a los ciberdelincuentes acceder a información privilegiada de los usuarios. También se sugiere que estas plataformas brinden capacitación continua a los usuarios a través de programas de formación, ya que esto contribuirá a prevenir actividades ilícitas.

REFERENCIAS

7.1. Fuentes documentales

- Amores, L. (2022). *La falta de tipificación del delito informático “sexting” dentro del COIP y su vulneración a los derechos de la dignidad humana e intimidad en el Ecuador*. (Tesis pregrado). Universidad Regional Autónoma de los Andes, Riobamba, Ecuador: Repositorio institucional UNIANDES. Disponible en: <https://dspace.uniandes.edu.ec/bitstream/123456789/14490/1/UR-DER-PDI-072-2022.pdf>.
- Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos*. (Tesis pregrado). Universidad César Vallejo, Trujillo, Perú: Repositorio institucional UCV. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/80920/Aredo_LLA-SD.pdf?sequence=1&isAllowed=y.
- Cuñas, E. (2021). *Los datos personales en las redes sociales y el derecho a la intimidad personal*. (Tesis pregrado). Universidad Regional Autónoma de los Andes : Repositorio institucional UNIANDES. Disponible en: <https://dspace.uniandes.edu.ec/bitstream/123456789/13735/1/UR-DER-PDI-031-2021.pdf>.
- Jacobo, J., & Quispe, K. (2019). *Delitos informáticos orientados en casos de violación a la intimidad en el ámbito sexual de Lima Metropolitana-2018*. (Tesis pregrado). Universidad Autónoma del Perú, Lima, Perú: Repositorio institucional AUTONOMA. Disponible en: <https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/1348/Jacobo%20Aquino%2c%20Jose%20Mauricio%20y%20Quispe%20Ochoa%2c%20Karina.pdf?sequence=1&isAllowed=y>.
- Muñoz, L. (2018). *Protección penal de la intimidad personal en las redes sociales*. (Tesis pregrado). Universidad Nacional del Altiplano, Puno, Perú: Repositorio institucional UNAP. Disponible en: <https://renati.sunedu.gob.pe/handle/sunedu/3226875>.
- Palacios, E. (2021). *Los delitos informáticos contra datos, y su vulneración al derecho de la intimidad personal, en la ciudad de Ayacucho, 2020*. (Tesis pregrado). Universidad César Vallejo, Lima, Perú: Repositorio institucional UCV. Disponible en: <https://repositorio.ucv.edu.pe/handle/20.500.12692/74705>.

- Pérez, C. (2022). *Los delitos informáticos y el derecho a la intimidad personal*, Lima Metropolitana, 2021. (Tesis pregrado). Universidad César Vallejo, Lima, Perú: Repositorio institucional UCV. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/113044/Perez_CCDP-SD.pdf?sequence=1&isAllowed=y.
- Ruiz, C. (2016). *Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos*. (Tesis pregrado). Universidad Nacional de Loja, Loja, Ecuador:: Repositorio institucional UNL. Disponible en: <https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf>.
- Torres, J. (2022). *El derecho a la intimidad de la persona pública y el perjuicio moral, en la provincia de Huaral*. (Tesis Maestría). Universidad Inca Garcilaso de la Vega, Lima, Perú: Repositorio institucional UIGV. Disponible en: http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/6041/TESIS_TORRES%20GUERRA.pdf?sequence=1&isAllowed=y.
- Urpeque, C. (2019). *Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos*. Huaura 2018. (Tesis pregrado). Universidad Nacional José Faustino Sánchez Carrión, Huacho, Perú: Repositorio institucional UNJFSC. Disponible en: <https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/4632/Cristian%20Jos%c3%a9%20Urpeque%20Tarazona.pdf?sequence=1&isAllowed=y>.
- Zamora, J. (2020). *Los delitos informáticos y el derecho a la intimidad en el Código Orgánico Integral Penal*. (Tesis pregrado). Universidad Técnica de Ambato, Ambato, Ecuador: Repositorio institucional UTA. Disponible en: <https://repositorio.uta.edu.ec/bitstream/123456789/31564/1/BJCS-DE-1147.pdf>.
- Zarate, C. (2023). *La vulneración del derecho a la intimidad personal en el uso de las redes sociales en los jóvenes en la Provincia de Bagua en el año 2021*. (Tesis pregrado). Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, Chachapoyas, Perú: Repositorio institucional UNTRM. Disponible en: <https://repositorio.untrm.edu.pe/bitstream/handle/20.500.14077/3156/Zarate%20Polo%20Carlos%20Rodrigo.pdf?sequence=3&isAllowed=y>.

7.2. Fuentes bibliograficas

- Bernal, C. (2012). *Metodología de la Investigación. 3ra Edición*. México: Pearson.
 Disponible en: <https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf>.
- Chenet, M. (2018). *Metodología de investigación científica universitaria: Guía para la elaboración del proyecto de tesis (Primera ed)*. Perú: Editorial Soluciones Gráficas. Disponible en: <https://isbn.cloud/9786124760167/metodologia-de-investigacion-cientifica-universitaria/>.
- Código Civil. (2021). *Decreto Legislativo 295*. Lima: Jurista Editores E.I.R.L.
- Ford, E. (2015). *El reto de la democracia digita. Hacia una ciudadanía interconectada*. Lima: Tarea Asociación Gráfica Educativa. Disponible en: <https://www.kas.de/documents/269552/269601/El+reto+de+la+democracia+digital+hacia+una+ciudadan%C3%ADa+interconectada.pdf/3c571428-98b1-c3b7-c47c-63cc5fb715ef?version=1.2&t=1574964153718>.
- García, A. (2015). *Derecho penal y redes sociales*. Madrid: Aranzadi.
- Hernandez, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación. 6ta Edicion*. México: McGraw-Hill Interamericana. Disponible en: <https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Methodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf>.
- Kurbalija, J. (2016). *An Introduction to Internet Governance (7a Ed.)*. Ginebra : DIPLOFoundation. Disponible en: https://issuu.com/diplo/docs/ig2016_7th_ed_esp.
- Peña, O., y Almanza, F. . (2010). *Teoria del delito (Manual Practico para su aplicacion en la Teoria de casos)*. Lima: APECC. Disponible en: <https://derecho.usmp.edu.pe/wp-content/uploads/2022/05/libro-teoria-del-delito-oscar-pena.pdf>.
- Silva, J. (1992). *Aproximación al derecho penal contemporáneo*. Barcelona: J. M. Bosch Editor.

7.3. Fuentes hemerográficas

- Arellano, C. (2021). El derecho de protección de datos personales. *Biolex*, 12(23), 163-174. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S2007-55452020000200009&script=sci_arttext.
- Arellano, W., & Ochoa, A. (2013). Derechos de privacidad e información en la sociedad de la información y en el entorno TIC. *Revista Ius*, 7(31), 183-206. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1870-21472013000100010&script=sci_arttext.
- Baño, Á., & Reyes, J. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. *Revista jurídica crítica y derecho*, 1(1), 49-60. Disponible en: <https://revistadigital.uce.edu.ec/index.php/criticayderecho/article/view/2447/2518>.
- Castro, Á. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. *Novum Jus*, 10(1), 113-133. Disponible en: <https://novumjus.ucatolica.edu.co/article/view/1178>.
- Constitución Política del Perú. (1993). *Constitución Política del Perú de 1993*. Lima: Diario El Peruano.
- Fusco, L. (2020). Los delitos informáticos en el Código Penal Italiano. *Derecho global. Estudios sobre derecho y justicia*, 5(14), 127-149. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S2448-51362020000100105&script=sci_arttext.
- Han, C., y Dongre, R. (2014). ¿Qué motiva a los ciber-atacantes? *Revista de la gestión de la innovación tecnológica*, 4(10). 40-42.
- Horn, A. (2021). ¿Qué ideas sobre su derecho a la intimidad en la escuela construyen niños y niñas? *Educação e Pesquisa*, 47. Disponible en: <http://educa.fcc.org.br/pdf/ep/v47/1517-9702-ep-47-e237848.pdf>.
- Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, 44(1), 261-285. Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_arttext&tlng=pt.
- Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, 44(1), 261-285. Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_arttext&tlng=pt.

- Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis*, 24(1), 159-206. Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext.
- Pfeffer, E. (2000). Los derechos a la intimidad o privacidad, a la honra ya la propia imagen. Su protección frente a la libertad de opinión e información. *Revista Ius et Praxis*, 6(1), 465-474. Disponible en: <https://www.redalyc.org/pdf/197/19760123.pdf>.
- Salvador, W. (2022). *Derecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicos en víctimas ecuatorianas*. 3(9), 41-55. Disponible en: <https://mundofinanciero.indecsar.org/revista/index.php/munfin/article/view/74/79: Revista Mundo Financiero>.
- Villavicencio, F. (2014). Delitos informáticos. *IUS ET VERITAS*, (49), 284-304.

7.4. Fuentes electrónicas

- BCN. (2022). *Ley Fácil*. Obtenido de <https://www.bcn.cl/portal/leyfacil/recurso/delitos-informaticos>
- Defensoria del Pueblo. (4 de abril de 2019). *Ordenan a Google retirar datos personales de mujer víctima de violación a la intimidad personal*. Obtenido de <https://www.defensoria.gob.pe/ordenan-a-google-retirar-datos-personales-de-mujer-victima-de-violacion-a-la-intimidad-personal/>
- El Consejo de Derechos Humanos. (2018). *Promoción, protección y disfrute de los derechos humanos en Internet*. Obtenido de https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf
- Enciclopedia Etecé. (2023). *Dato en informática*. Obtenido de [https://concepto.de/dato-en-informatica/#:~:text=Informaci%C3%B3n%20\(en%20inform%C3%A1tica\)-,%C2%BFQu%C3%A9%20es%20un%20dato%3F,%2C%20un%20suceso%2C%20una%20entidad](https://concepto.de/dato-en-informatica/#:~:text=Informaci%C3%B3n%20(en%20inform%C3%A1tica)-,%C2%BFQu%C3%A9%20es%20un%20dato%3F,%2C%20un%20suceso%2C%20una%20entidad).
- ISOC. (2015). *Internet Society: Dando forma a Internet. Historia y futuro*. Obtenido de <https://www.kas.de/documents/269552/269601/El+reto+de+la+democracia+digital+hacia+una+ciudadan%C3%ADa+interconectada.pdf/3c571428-98b1-c3b7-c47c-63cc5fb715ef?version=1.2&t=1574964153718>

ANEXOS

Anexo 1: Matriz de consistencia
DELITOS INFORMÁTICOS Y LA VULNERACIÓN AL DERECHO A LA INTIMIDAD PERSONAL EN LA PROVINCIA DE BARRANCA, 2023

Problema	Objetivos	Hipótesis	Variables	Indicadores	Metodología
<p>Problema General ¿Cómo los delitos informáticos contra los datos influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023?</p> <p>Problema Específicos 1) ¿Cómo los delitos informáticos contra los datos influyen en la vulneración de la intimidad personal en la provincia de Barranca en el año 2023? 2) ¿Cómo los delitos informáticos contra los datos influyen en la vulneración de la privacidad personal en la provincia de Barranca en el año 2023? 3) ¿Cómo los delitos informáticos contra los datos influyen en la vulneración de la reserva personal en la provincia de Barranca en el año 2023?</p>	<p>Objetivo General Determinar la influencia de los delitos informáticos contra los datos sobre la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023.</p> <p>Objetivos Específicos 1) Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la intimidad personal en la provincia de Barranca en el año 2023. 2) Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la privacidad personal en la provincia de Barranca en el año 2023. 3) Establecer la influencia de los delitos informáticos contra los datos sobre la vulneración de la reserva personal en la provincia de Barranca en el año 2023.</p>	<p>Hipótesis General Los delitos informáticos contra los datos influyen en la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023.</p>	<p>Variable X: Delitos informáticos</p> <p>Dimensiones</p> <ul style="list-style-type: none"> • Sistemas informáticos X₁ • Datos informáticos X₂ • Acceso ilícito X₃ <p>Variable Y: Derecho a la intimidad personal</p> <ul style="list-style-type: none"> • Intimidad Y₁ • Privacidad Y₂ • Reserva Y₃ 	<p>X_{1.1}. Datos personales X_{1.2}. Uso de software X_{1.3}. Uso de hardware</p> <p>X_{2.1}. Almacenamientos X_{2.2}. Procedimientos X_{2.3}. Aplicaciones</p> <p>X_{3.1}. Vulneración X_{3.2}. Intromisión X_{3.3}. Extracción</p> <p>Y_{1.1}. Vulnerar Y_{1.2}. Resarcir Y_{1.3}. Afectar</p> <p>Y_{2.1}. Atentar Y_{2.2}. Formular Y_{2.3}. Limitar</p> <p>Y_{3.1}. Alteración Y_{3.2}. Capacidad Y_{3.3}. Indemnizar</p>	<p>Población: 60 personas</p> <p>Muestra: 28 personas</p> <p>Nivel de Investigación: Correlacional</p> <p>Tipo de Investigación: Descriptiva</p> <p>Diseño: No experimental</p> <p>Instrumentos: Cuestionario de 25 ítems para la variable X y 20 ítems para la variable Y Entrevista de 12 ítems</p>

Anexo 2: Instrumentos



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

CUESTIONARIO

A. Presentación

Estimado Sr. o Sra., este cuestionario forma parte de una investigación cuyo propósito es recopilar información sobre "Delitos informáticos y la vulneración al derecho a la intimidad personal en la provincia de Barranca en el año 2023". Su opinión personal es de gran importancia para nuestro estudio.

B. Indicaciones

- Este cuestionario se mantendrá anónimo. Le pedimos que responda con total sinceridad.
- Lea atentamente cada pregunta. Cada una de ellas ofrece cinco opciones de respuesta.
- Por favor, marque con una "X" en el recuadro correspondiente la opción que mejor refleje su opinión o describa el sistema de información de su institución.
- Cabe destacar que este instrumento se basa en una adaptación de un cuestionario desarrollado por Torres en 2022.
- La escala de calificación utilizada es la siguiente:

1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Ítem	Enunciados	1	2	3	4	5
1	El uso de las redes sociales no garantiza la seguridad de su privacidad de información.					
2	Las publicaciones que realiza en las redes o plataformas sociales son de fácil acceso para otros usuarios.					
3	Cuando otras personas publican fotos, videos, u otros contenidos sin su consentimiento, están violando su derecho a la intimidad personal.					
4	Las sanciones por la intromisión en la vida privada de otras personas a través de las redes sociales deberían ser más severas.					
5	La protección del derecho a la intimidad personal se basa en las leyes establecidas en nuestra constitución.					
6	Las leyes vigentes desempeñan un papel fundamental en la protección de su derecho a la intimidad al utilizar cualquier forma de comunicación digital.					
7	Aquellos que violan la intimidad de personas públicas deberían ser castigados de manera rigurosa.					
8	Deberían incrementarse las penas por la violación de los derechos a la intimidad de las personas.					
9	Es necesario realizar modificaciones en el código civil y penal para lograr una mayor justicia para quienes ven afectados su honor, su imagen o su vida privada.					
10	Los medios de comunicación a veces abusan de su derecho a la libertad de expresión al difundir aspectos íntimos de las personas.					
11	Se considera que las personas públicas no cuentan con una protección adecuada en lo que respecta a su intimidad personal.					
12	La vulneración de la intimidad de una persona puede tener un impacto perjudicial en su entorno familiar o social.					



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

GUÍA DE ENTREVISTA – ESPECIALISTAS

Sr. Especialista, la presente entrevista tiene por finalidad de recopilar su opinión respecto a los **“Delitos informáticos y la vulneración al derecho a la intimidad personal en la provincia de Barranca, 2023”**. Agradezco su tiempo y colaboración.

1. ¿De qué forma los delitos informáticos contra los datos vulneran el derecho a la intimidad personal?

Opinión:

.....

.....

.....

.....

.....

2. ¿Cuáles son las consecuencias que conlleva los delitos informáticos en la vulneración del derecho a la intimidad personal?

Opinión:

.....

.....

.....

.....

.....

3. ¿Se aplican adecuadamente las sanciones penales en coherencia al accionar de este tipo de delito informático, las cuales atentan al derecho a la intimidad personal?

Opinión:

.....

.....

.....

.....
.....

4. ¿Los Delitos Informáticos, se han convertido en una nueva forma de atentar y vulnerar la intimidad de las personas a través del uso de la tecnología en la provincia de Barranca?

Opinión:

.....
.....
.....
.....
.....

5. ¿Cómo el derecho a la intimidad personal garantiza el resarcimiento del daño?

Opinión:

.....
.....
.....
.....
.....

6. ¿Considera que este tipo de delitos a nivel tecnológico afecta psicológicamente a la víctima?

Opinión:

.....
.....
.....
.....
.....

7. ¿Consideraría usted que los delitos informáticos de datos, atenta contra la privacidad personal de los ciudadanos de la provincia de Barranca, mediante el uso de la tecnología?

Opinión:

.....

.....
.....
.....
.....

8. ¿Es necesario la formulación de medidas o acciones de nivel tecnológico para frenar este tipo de delitos informáticos según los avances tecnológicos?

Opinión:

.....
.....
.....
.....
.....

9. ¿Consideraría usted que existen límites en el desarrollo de un delito informático hacia la privacidad personal en la provincia de Barranca?

Opinión:

.....
.....
.....
.....
.....

10. ¿Los delitos informáticos pueden ocasionar una alteración o una usurpación en los datos de las víctimas, a través de las redes sociales en la provincia de Barranca?

Opinión:

.....
.....
.....
.....
.....

11. ¿Incrementar la capacitación o actualizar a los operadores del derecho, en la defensa de las víctimas de este tipo de delitos informáticos, generara una efectividad de las sanciones en la provincia de Barranca?

Opinión:

.....
.....
.....
.....
.....

12. ¿Consideraría usted que los medios informáticos son un daño indemnizable?

Opinión:

.....
.....
.....
.....
.....

Anexo 3: Confiabilidad de los instrumentos



UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

DELITOS INFORMÁTICOS

Prueba Coeficiente alfa de Cronbach:

La confiabilidad del cuestionario se estimó a través de la Prueba Coeficiente alfa de Cronbach, la ventaja de este coeficiente reside en que requiere de una sola administración del instrumento de medición. Puede tomar valores entre 0 y 1, donde 0 significa confiabilidad nula y 1 representa la confiabilidad total.

Estadístico de fiabilidad

<i>Estadísticas de fiabilidad</i>	
Alfa de Cronbach	N de elementos
,624	6

<i>Estadísticas de fiabilidad</i>	
Alfa de Cronbach	N de elementos
,637	6



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

Anexo 4: Base de datos

IBM SPSS Statistics: Editor de datos

Archivo Editor Ver Datos Transformar Analizar Gráficos Librerías Aplicaciones Ventanas Ayuda

Visible: 16 de 16 variables

	VAR1DIM1 F001	VAR1DIM1P 002	VAR1DIM2 F003	VAR1DIM2 2F004	VAR1DIM3 F005	VAR1DIM3P 006	VAR2DIM1 F001	VAR2DIM1P 002	VAR2DIM2 F003	VAR2DIM2P 04	VAR2DIM3P 005	VAR2DIM3P0 06	VAR1
1	5	5	4	4	4	3	5	3	5	5	4	4	25
2	4	6	6	4	6	6	6	6	6	5	5	4	28
3	4	4	4	3	4	5	5	5	4	4	4	3	24
4	5	5	5	4	5	5	5	5	5	5	5	4	29
5	4	4	4	3	4	4	5	4	4	4	4	3	23
6	5	5	5	3	6	5	5	5	5	5	5	3	28
7	4	4	4	6	4	5	6	4	4	4	4	5	27
8	5	5	5	5	4	4	4	4	4	5	5	5	28
9	4	3	3	3	4	5	5	5	3	3	3	4	24
10	5	5	5	4	4	3	5	3	5	5	5	4	26
11	3	4	4	3	6	3	6	3	6	4	4	3	22
12	5	5	3	4	4	4	4	4	4	5	3	4	25
13	2	2	2	3	6	6	2	6	2	2	2	3	19
14	5	5	4	5	4	4	2	4	2	5	5	5	27
15	4	6	4	2	6	6	6	6	6	6	6	2	26
16	5	5	4	3	4	5	5	5	5	5	5	3	26
17	6	6	4	4	2	6	6	6	6	6	6	4	25
18	4	1	1	1	2	5	5	5	1	1	1	1	14
19	5	4	6	4	3	2	3	2	4	5	4	4	23
20	4	4	4	4	4	3	2	2	3	4	4	4	21
21	1	3	3	4	3	3	5	3	5	3	3	4	17
22	4	4	5	2	4	1	1	1	1	5	5	2	21

Vista de datos | Vista de variables

IBM SPSS Statistics: Procesador de lista | Unidad: ON | 6:26 p.m. | 12/07/2023

Anexo 5: Evidencia fotográfica



