



**Autónoma**  
Universidad Autónoma del Perú

**FACULTAD DE DERECHO  
ESCUELA PROFESIONAL DE DERECHO**

**Tesis**  
**LAS CONSECUENCIAS DEL CARDING EN LA  
PROTECCIÓN DE DATOS PERSONALES, LIMA  
METROPOLITANA, 2024**

**PARA OBTENER EL TÍTULO DE  
ABOGADO**

**Autores**

BREÑA RAMÍREZ, Christian Manuel (ORCID: 0000-0001-5967-4630)  
LLONTOP VILLON, Brenda Zarela (ORCID: 0000-0002-8968-3658)  
MANCO RAMÍREZ, Jusan Enrique Junior (ORCID: 0000-0002-2023-  
5304)

**Asesor**

MAG. AYBAR YZAGUIRRE, Gerardo Manuel (ORCID:0000-0003-3547-  
7602)

**Línea de investigación del programa**  
Enfoque interdisciplinario de la ciencia jurídica

**Línea de acción RSU**  
Salud y bienestar

**LIMA, PERÚ, ABRIL DE 2025**



**CC BY**

<https://creativecommons.org/licenses/by/4.0/>

*Esta licencia permite a otros distribuir, mezclar, ajustar y construir a partir de su obra, incluso con fines comerciales, siempre que le sea reconocida la autoría de la creación original. Esta es la licencia más servicial de las ofrecidas. Recomendada para una máxima difusión y utilización de los materiales sujetos a la licencia.*

## Referencia bibliográfica

Breña Ramírez, C. M., Llontop Villon, B. Z., & Manco Ramírez, J. E. J. (2025). *Las consecuencias del carding en la protección de datos personales Lima Metropolitana 2024* [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

## HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Christian Manuel Breña Ramírez
Tipo de documento de identidad	DNI
Número de documento de identidad	73759318
URL de ORCID	<a href="https://orcid.org/0000-0001-5967-4630">https://orcid.org/0000-0001-5967-4630</a>
Datos del autor	
Nombres y apellidos	Brenda Zarela Llontop Villon
Tipo de documento de identidad	DNI
Número de documento de identidad	75495730
URL de ORCID	<a href="https://orcid.org/0000-0002-8968-3658">https://orcid.org/0000-0002-8968-3658</a>
Datos del autor	
Nombres y apellidos	Jusan Enrique Junior Manco Ramírez
Tipo de documento de identidad	DNI
Número de documento de identidad	76361676
URL de ORCID	<a href="https://orcid.org/0000-0002-2023-5304">https://orcid.org/0000-0002-2023-5304</a>
Datos del asesor	
Nombres y apellidos	Gerardo Manuel Aybar Yzaguirre
Tipo de documento de identidad	DNI
Número de documento de identidad	44823980
URL de ORCID	<a href="https://orcid.org/0000-0003-3547-7602">https://orcid.org/0000-0003-3547-7602</a>
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Carlos Antonio Agurto Gonzáles
Tipo de documento	DNI
Número de documento de identidad	42378796
Secretario del jurado	
Nombres y apellidos	Luis Angel Espinoza Pajuelo
Tipo de documento	DNI
Número de documento de identidad	10594662
Vocal del jurado	

<b>Nombres y apellidos</b>	María Pía Díaz Díaz
<b>Tipo de documento</b>	DNI
<b>Número de documento de identidad</b>	45484099
<b>Datos de la investigación</b>	
<b>Título de la investigación</b>	Las consecuencias del carding en la protección de datos personales Lima Metropolitana 2024
<b>Línea de investigación Institucional</b>	Persona, Sociedad, Empresa, Estado
<b>Línea de investigación del Programa</b>	Enfoque interdisciplinario de la ciencia jurídica
<b>Línea de acción RSU</b>	Salud y bienestar
<b>URL de disciplinas OCDE</b>	<a href="https://purl.org/pe-repo/ocde/ford#5.05.01">https://purl.org/pe-repo/ocde/ford#5.05.01</a>

**FACULTAD DE DERECHO**  
**ESCUELA PROFESIONAL DE DERECHO**  
**ACTA DE SUSTENTACIÓN DE TESIS**

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: el DR. CARLOS ANTONIO AGURTO GONZALES como presidente, el DR. LUIS ANGEL ESPINOZA PAJUELO como secretario y la DRA. MARÍA PÍA DIAZ DIAZ como vocal, reunidos en acto público para dictaminar la tesis titulada:

**LAS CONSECUENCIAS DEL CARDING EN LA PROTECCIÓN DE DATOS  
PERSONALES LIMA METROPOLITANA 2024**

Presentado por el bachiller:

**CRHISTIAN MANUEL BREÑA RAMIREZ**

Para obtener el **Título Profesional de Abogado**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado-Bueno** con una calificación de **DIECISÉIS (16)**.

En fe de lo cual firman los miembros del jurado, el 23 de abril de 2025



**PRESIDENTE**  
DR. CARLOS ANTONIO  
AGURTO GONZALES



**SECRETARIO**  
DR. LUIS ANGEL ESPINOZA  
PAJUELO



**VOCAL**  
DRA. MARÍA PÍA DIAZ DIAZ

**FACULTAD DE DERECHO**  
**ESCUELA PROFESIONAL DE DERECHO**  
**ACTA DE SUSTENTACIÓN DE TESIS**

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: el DR. CARLOS ANTONIO AGURTO GONZALES como presidente, el DR. LUIS ANGEL ESPINOZA PAJUELO como secretario y la DRA. MARÍA PÍA DIAZ DIAZ como vocal, reunidos en acto público para dictaminar la tesis titulada:

**LAS CONSECUENCIAS DEL CARDING EN LA PROTECCIÓN DE DATOS**  
**PERSONALES LIMA METROPOLITANA 2024**

Presentado por la bachiller:

**BRENDA ZARELA LLONTOPI VILLON**

Para obtener el **Título Profesional de Abogada**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado-Bueno** con una calificación de **DIECISÉIS (16)**.

En fe de lo cual firman los miembros del jurado, el 23 de abril de 2025



**PRESIDENTE**  
DR. CARLOS ANTONIO  
AGURTO GONZALES



**SECRETARIO**  
DR. LUIS ANGEL ESPINOZA  
PAJUELO



**VOCAL**  
DRA. MARÍA PÍA DIAZ DIAZ

**FACULTAD DE DERECHO**  
**ESCUELA PROFESIONAL DE DERECHO**  
**ACTA DE SUSTENTACIÓN DE TESIS**

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: el DR. CARLOS ANTONIO AGURTO GONZALES como presidente, el DR. LUIS ANGEL ESPINOZA PAJUELO como secretario y la DRA. MARÍA PÍA DIAZ DIAZ como vocal, reunidos en acto público para dictaminar la tesis titulada:

**LAS CONSECUENCIAS DEL CARDING EN LA PROTECCIÓN DE DATOS**  
**PERSONALES LIMA METROPOLITANA 2024**

Presentado por el bachiller:

**JUSAN ENRIQUE JUNIOR MANCO RAMIREZ**

Para obtener el **Título Profesional de Abogado**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado-Bueno** con una calificación de **DIECISIETE (17)**.

En fe de lo cual firman los miembros del jurado, el 23 de abril de 2025



**PRESIDENTE**  
DR. CARLOS ANTONIO  
AGURTO GONZALES



**SECRETARIO**  
DR. LUIS ANGEL ESPINOZA  
PAJUELO



**VOCAL**  
DRA. MARIA PIA DIAZ DIAZ

## **ACTA DE APROBACIÓN DE ORIGINALIDAD**

Yo Gerardo Manuel Aybar Yzaguirre docente de la Facultad de Derecho de la Escuela Profesional de Derecho de la Universidad Autónoma del Perú, en mi condición de asesor de la tesis titulada:

### **LAS CONSECUENCIAS DEL CARDING EN LA PROTECCION DE DATOS PERSONALES, LIMA METROPOLITANA, 2024**

De los bachilleres Jusan Enrique Junior Manco Ramírez, Brenda Zarela Llontop Villon, Christian Manuel Breña Ramírez, certifico que la tesis tiene un índice de similitud de 15% verificable en el reporte de similitud del software Turnitin que se adjunta.

El suscrito examinó y evaluó el mencionado reporte, concluyendo que ninguna de las coincidencias identificadas representa un caso de plagio. Según su criterio profesional, la tesis cumple plenamente con las normas de citas y referencias estipuladas por la Universidad Autónoma del Perú.

Lima 14 de marzo de 2025



GERARDO MANUEL AYBAR YZAGUIRRE

DNI N° 44823980

**DEDICATORIA**

Esta tesis, la dedico a mis padres por su apoyo.

Christian Manuel Breña Ramírez

Dedica esta tesis a mis padres, amigos y asesor de tesis por su apoyo.

Brenda Zarela Llontop Villon

Dedica a mis padres y docentes por las enseñanzas vertidas a mi persona.

Jusan Enrique Junior Manco Ramírez

### **AGRADECIMIENTOS**

A mi abuela por sus enseñanzas sobre la independencia y la moralidad. A mi abuelo por enseñarme el valor del criterio propio, la lectura, el buen decir y el buen escribir; tus acciones fueron las mejores palabras. Y a mi compañera de vida por su lealtad, comprensión y compromiso conmigo y el producto de nuestro amor, Enrique.

Jusan Enrique Junior Manco Ramírez

A mis padres por su continuo esfuerzo e impulso para seguir adelante, a mi hermano por su gran apoyo y preocupación para continuar cumpliendo mis metas, a mis grandes amigos por ser las personas que me animan a investigar y explorar el Derecho.

Christian Manuel Breña Ramírez

A mis padres por su apoyo continuo, a Camilo por su leal compañía, a mis amistades por sus valiosos aportes.

Brenda Zarela Llontop Villon

**INDICE**

<b>DEDICATORIA</b> .....	<b>2</b>
<b>AGRADECIMIENTOS</b> .....	<b>3</b>
<b>LISTA DE TABLAS</b> .....	<b>5</b>
<b>RESUMEN</b> .....	<b>6</b>
<b>ABSTRACT</b> .....	<b>7</b>
<b>1. INTRODUCCIÓN</b> .....	<b>8</b>
<b>2. MÉTODO</b> .....	<b>18</b>
2.1 Tipo y diseño de investigación .....	18
2.2 Población, muestra y muestreo .....	19
2.3 Hipótesis .....	19
2.4 Variables y operacionalización .....	19
2.5 Técnicas e instrumentos de recolección de datos, validez y confiabilidad ...	20
2.6 Procedimientos .....	20
2.7 Análisis de datos .....	20
2.8 Aspectos éticos .....	21
<b>3. RESULTADOS</b> .....	<b>22</b>
<b>4. DISCUSIÓN</b> .....	<b>29</b>
<b>5. CONCLUSIONES</b> .....	<b>32</b>
<b>6. RECOMENDACIONES</b> .....	<b>33</b>
<b>REFERENCIAS</b> .....	<b>34</b>
<b>ANEXOS</b>	

**LISTA DE TABLAS**

Tabla 1	Muestra procesada
Tabla 2	Fiabilidad obtenida
Tabla 3	Fiabilidad de cada ítem
Tabla 4	Estadística del ítem N° 1
Tabla 5	Estadística del ítem N° 2
Tabla 6	Estadística del ítem N° 3
Tabla 7	Estadística del ítem N° 4
Tabla 8	Estadística del ítem N° 5
Tabla 9	Estadística del ítem N° 6
Tabla 10	Estadística del ítem N° 7
Tabla 11	Estadística del ítem N° 8
Tabla 12	Estadística del ítem N° 9
Tabla 13	Estadística del ítem N° 10
Tabla 14	Rangos estadísticos que esclarecen el contraste de la hipótesis general
Tabla 15	Rangos estadísticos que esclarecen el contraste de la hipótesis específica 1
Tabla 16	Rangos estadísticos que esclarecen el contraste de la hipótesis específica 12

**LAS CONSECUENCIAS DEL CARDING EN LA PROTECCIÓN DE DATOS  
PERSONALES EN LIMA METROPOLITANA 2024**

**CHRISTIAN MANUEL BREÑA RAMÍREZ**

**BRENDA ZARELA LLONTOP VILLON**

**JUSAN ENRIQUE JUNIOR MANCO RAMIREZ**

**UNIVERSIDAD AUTÓNOMA DEL PERÚ**

**RESUMEN**

El informe final se ha basado en la problemática en cuanto el tráfico y uso no autorizado de tarjetas de crédito conocido como carding y sus consecuencia en la vulneración de datos personales; en todo caso se ha tenido como objetivo respecto de la investigación en determinar la relación del carding con la protección de los datos personales en Lima Metropolitana; asimismo las consecuencias con los usuarios del sistema financiero y las mismas entidades bancarias; en este sentido se ha utilizado la metodología del enfoque cuantitativo como una de las formas que establece la guía académica, se ha utilizado el tipo básico por ser un trabajo eminentemente teórico, de diseño no experimental, por el hecho de no modificar variables y sólo observarlo en la realidad social, que se ha validado un instrumento conocido como cuestionario y se ha ejecutado por la cual se ha tenido la siguiente conclusión de que existe sí relación de manera directa entre la modalidad de fraude cibernético conocida como carding y la protección de los datos personales de los sujetos afectados.

***Palabras clave:*** delitos informáticos, datos personales, carding, conducta

**THE CONSEQUENCES OF CARDING IN THE PROTECTION OF PERSONAL  
DATA IN METROPOLITAN LIMA 2024**

**CHRISTIAN MANUEL BREÑA RAMÍREZ**

**BRENDA ZARELA LLONTOP VILLON**

**JUSAN ENRIQUE JUNIOR MANCO RAMIREZ**

**UNIVERSIDAD AUTÓNOMA DEL PERÚ**

**ABSTRACT**

The final report is based on the problem of unauthorized credit card trafficking and use, known as carding, and its consequences for the violation of personal data. The research objective was to determine the relationship between carding and the protection of personal data in Metropolitan Lima, as well as the consequences for users of the financial system and the banking entities themselves. In this regard, the quantitative approach methodology was used as one of the methods established by the academic guide. The basic type was used because it is an eminently theoretical work, with a non-experimental design, due to the fact that variables are not modified and it is only observed in social reality. A questionnaire was validated and executed, leading to the following conclusion: a direct relationship exists between the cyber fraud modality known as carding and the protection of personal data of the affected subjects.

**Keywords:** computer crimes, personal data, carding, conduct

## 1. INTRODUCCIÓN

El análisis del carding como ciberdelito evidencia un fenómeno global que refleja las profundas transformaciones sociales, económicas y tecnológicas de la era digital. Sobre los ilícitos, que contemplan los virus hasta la suplantación de sitios web, violaciones diversas a las normas penales y delitos que vulneran la privacidad de datos personales y de derechos de autor, demuestran cómo el incremento en la dependencia tecnológica sobre la información y comunicación (TIC) apertura horizontes sobre los hechos ilícitos (Vinelli, 2021).

Con la evolución en las telecomunicaciones, y el auge en información, ha generado un impacto en la sociedad importante sobre el uso de información electrónica. Empero, el avance del mismo se empleó con fines ilícitos mediante delitos cibernéticos, teniendo como ejemplo el Carding (Hatta, 2022). Entonces, el carding consiste en el uso indebido de tarjetas de crédito o débito que, mediante el accionar fraudulento o sometiendo a error a las personas, constituye un peligro sobre la seguridad económica de las víctimas, además de provocar pérdidas en instituciones financieras y de comercio electrónico (Amaiquema, 2023).

De acuerdo con Arévalo y Vega (2022) el carding ha evolucionado con la ayuda de las nuevas herramientas tecnológicas, las cuales permiten que los datos sensibles, puedan ser extraídos a través de diversas técnicas, lo cual pone en evidencia la constante adaptación de los ciberdelincuentes.

De esta forma, se ha provocado grandes perjuicios económicos al punto de ser devastadores, tanto para víctimas, instituciones financieras y comercios electrónicos a través del carding. Sagala et al. (2025) ha indicado que este ciberdelito ha generado pérdidas económicas por más de miles de millones de dólares. Así también, Trucios (2023) precisó que la afectación no es solamente para la estabilidad económica de las víctimas, sino que mella en la confianza de los consumidores digitales.

Las malas experiencias y la desconfianza sobre la posibilidad de la vulneración de datos, ha provocado un estancamiento en la absorción tecnológica por parte de la población y de igual forma una dificultad en el crecimiento de los comercios electrónicos, considerando especialmente los países en desarrollo con infraestructuras de ciberseguridad insuficientes (Ocupa, 2022).

El impacto del carding ha generado un gran perjuicio en la sociedad al provocar el incremento de la desconfianza en el uso de tecnologías digitales, pues quienes son víctimas no solo pierden dinero, sino también les aumenta la sensación de

vulnerabilidad y desamparo, que puede llevar a una resistencia a adoptar servicios digitales (Defensoría del Pueblo, 2023). Adicionalmente, se ha reflejado que, en la sociedad, las personas con menor acceso a educación tecnológica o con los medios para protegerse, son más propensos a la vulneración. De acuerdo con Alcalá y Meléndez (2023) se ha demostrado la existencia de una brecha y se ha fortalecido la perspectiva que no existe tecnología moderna segura ni accesible para todos.

Existe una descomposición de la ética social, en donde se percibe impunidad y accesibilidad a beneficios ilícitos en este tipo de actividades, lo cual menoscaba los valores de integridad y respeto a los derechos (Defensoría del Pueblo, 2023). Como afirmó Sánchez (2020) este fenómeno no solo afectó a los directamente involucrados, sino que también contribuye a la normalización de conductas contra la norma en el entorno digital, ampliando el alcance de la ciberdelincuencia y complicando aún más los esfuerzos para garantizar la protección y la seguridad en cuanto al uso de las tecnologías.

Ante ello, la pregunta general planteada es ¿En qué medida el carding se relaciona con la protección de datos personales en Lima Metropolitana 2024? Asimismo, la pregunta específica uno precisa lo siguiente: ¿en qué medida el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados? también en el caso de la pregunta específica dos dice: ¿en qué medida el tráfico de tarjetas de crédito se relaciona con el agravio de las entidades empresariales que prestan servicios por internet?

El carding es un desafío multifacético que requiere la combinación de legislación actualizada, educación digital, innovación tecnológica y cooperación internacional, en un mundo cada vez más interconectado, proteger derechos constitucionales garantizados por el Estado de Derecho como la privacidad y la seguridad de datos personales no solo es una necesidad legal, sino también un imperativo ético y social. Se tiene que dar prioridad a una cultura con ciberseguridad sólida, en la que, las políticas públicas adaptativas sean primordiales para la reducción de las problemáticas, prevaleciendo así el entorno digital seguro y con la búsqueda del desarrollo.

En México, se ha destacado que en la época de pandemia por el COVID-19, se incrementó la digitalización de sectores fundamentales como la salud y la educación. Lo cual ha generado un aumento de fraude informático mediante carding (Arévalo & Vega, 2022). Pese a ello, la legislación no tuvo un avance eficiente,

generando un vacío en la protección efectiva de los usuarios digitales. La inobservancia normativa penal ha provocado un estado de vulnerabilidad, que destaca la importancia del análisis y actualización de los marcos legales, con la finalidad de prevenir la comisión de delitos de manera eficaz (Zambrano, 2022).

Se ha demostrado la existencia de una necesidad sobre medidas preventivas y educativas para fortalecer las normas existentes.

Carriedo (2022) ha relacionado el delito de carding y los derechos humanos en México, destacando que la armonía de los derechos humanos con normas penales, puede proteger de manera más eficiente los datos personales de los usuarios, al tipificar y sancionar las conductas delictivas.

Paguay (2020) ha investigado el delito de carding con las compras en línea en Ecuador, lo cual tuvo como resultado que existen vacíos legales sobre el fraude digital, concluyendo en que, tanto compradores como vendedores pueden ser autores de delitos. Ello resalta la importancia de contar con normas actualizadas constantemente a fin de prevenir la falta de sanción y proteger la seguridad de los usuarios en actividades bancarias.

En el caso colombiano, estas cifras tienen un crecimiento exponencial. De acuerdo con Álvarez (2023), tan solo en el año 2022, se reportaron más de 54.000 denuncias por carding, siendo este un cambio significativo en relación a periodos anteriores. Principalmente estas modalidades incluyen fraudes financieros y robo de contraseñas, las cuales, mediante uso de ingeniería social, vulneran la seguridad de los usuarios.

Peña (2023) concluyó que, en el caso colombiano, las suplantaciones telefónicas, estadas y fraudes cibernéticos afectan a la economía y confianza de los usuarios debido al impacto que los ilícitos provocan. De esta manera, y con el impulso de la tecnología, se ha presionado al Estado sobre la implementación de nuevas medidas para tutelar los derechos de los ciudadanos y sancionar eficientemente a los delincuentes.

Según reportes del diario El Peruano (2023) en el Perú se ha evidenciado una creciente tendencia de denuncias, aproximadamente 300 al mes, sobre fraudes informáticos, representando la mitad de los casos registrados.

Por otro lado, la Defensoría del Pueblo (2023) determinó que Lima Metropolitana es la región con una mayor cantidad de casos por ciberdelitos, representando más del 53% de las denuncias policiales en el 2021. Refleja así, que

la población no cuenta con una adecuada educación digital y exponen información personal en las redes sociales y correos electrónicos, desconociendo los riesgos derivados de estas acciones.

De acuerdo con ello, en Perú se implementó en el año 2013, la Ley de Delitos Informáticos, con la finalidad de prevenir y sancionar los mismos. Aunque siendo importante su implementación, ello no fue suficiente para el nivel de sofisticación y dinamismo de los delincuentes, que hacen uso de las TIC, innovando métodos y mecanismos que superan barreras y borran rastros que los pudieran identificar. El verdadero desafío entonces, se encuentra en la capacidad de adaptación de las disposiciones convencionales a las particularidades locales, y la limitación respecto a la educación tecnológica, derivada de las restricciones presupuestarias en la implementación de tecnología avanzada.

Trucios (2023), en el Perú, ha abordado que los casos de carding se relaciona con la vulnerabilidad de los menores, al ser expuestos a medios de comunicación electrónicos utilizados con fines ilícitos, lo cual expone a los menores a la explotación laboral y sexual. Se resalta así la necesidad de la implementación de políticas públicas que puedan resguardar a los menores respecto a la problemática.

Según Ocupa (2022) el Convenio de Budapest en Perú tiene gran relevancia para el fortalecimiento de medidas para combatir la ciberdelincuencia mediante la tipificación y sanción del carding. Esta norma supranacional contribuyó con la cooperación internacional y generó cambios significativos en las normas peruanas en beneficio de la protección digital.

Por ello, Sotomayor (2022) investigó la calificación fiscal respecto al carding en el distrito fiscal de Lima Centro, en donde determinó que en gran medida estos ilícitos no son calificados adecuadamente durante el proceso, derivando en la desnaturalización de los hechos investigados, afectando la efectividad de las sanciones penales.

De este modo, Rodríguez (2020) indica que existe una necesidad de medidas integrales que aborden el carding para proteger a los usuarios y fortalezca la protección digital en contextos varios. Específicamente, en la constitucionalidad de la protección de datos personales.

Respecto a la variable carding, se manifiesta la complejidad de la ciberdelincuencia, la cual trasciende fronteras por su naturaleza global, afectando la seguridad financiera.

La dimensión ciberdelincuencia es definida como la actividad ilícita que emplea la tecnología avanzada para la comisión de delitos, como el carding, permitiendo operaciones más precisas, profesionales y anónimas. Como destacan Arévalo y Vega (2022), se incrementó a causa del uso de instrumentos tecnológicos avanzados y requiere de un marco regulatorio internacional más robusto y políticas de ciberseguridad coordinadas entre los Estados. Mientras que la dimensión seguridad financiera es referida al grupo de medidas y planes que tienen como fin la protección de instituciones financieras, consumidores y comercios digitales respecto a pérdidas económicas, así como los derivados de las actividades ilícitas como el carding.

Entre las modalidades delictivas más predominantes, se encuentran el uso de malware, técnicas de phishing y acceso no autorizado a estos sistemas; sin embargo, el impacto económico, financiero y social, afecta a víctimas, instituciones y ecosistemas digitales.

La protección de datos personales resulta fundamental en la sociedad digital actual, debido a la garantía sobre la información personal respecto a los usuarios. Ninasivincha y Gutierrez (2023) contemplan que este derecho constitucionalmente protegido, se encuentra relacionado con el ámbito privado personal, además de reforzar la confianza de las tecnologías, y de igual manera incentivando el desarrollo del comercio virtual y la interacción en este tipo de plataformas.

La dimensión afectación de datos personales, es referida al acceso, uso o divulgación sin la autorización de datos personales, provocando así grandes riesgos sobre la privacidad y seguridad de los individuos y/o usuarios en el contexto del carding.

La dimensión confianza colectiva está directamente relacionada con la generalización sobre la perspectiva de la seguridad y fiabilidad en el contexto digital, resultando importante para incentivar la interacción en plataformas electrónicas y desarrollando la economía digital de manera inclusiva.

Resulta importante destacar la relevancia que tiene el impacto social como dimensión clave respecto a la seguridad de los datos y los derechos fundamentales, pues en ello se descubre una vulneración en la confianza colectiva sobre la evolución de economías digitales.

Sauer (2024) también trató con la teoría absoluta de la pena, según la cual la justificación de la pena reside en la propia pena, desvinculada de cualquier bien futuro

o efecto social. Tal perspectiva entiende la pena como una respuesta justificada al crimen: la entidad en cuestión debe ser castigada, ya que el daño causado por un acto criminal no debe quedar sin atención.

Este concepto es importante dentro del contexto del carding, donde la ausencia de fronteras físicas y la intangibilidad de los bienes afectados presentan desafíos únicos para aplicar penas que reflejen adecuadamente la gravedad del daño causado.

Gaimari (2021) aborda la importancia de enfrentar nuevos retos de carácter políticos criminales frente a las nuevas formas delictivas y el ámbito social en el que las mismas se producen. Barahona (2023) indica que se ha estructurado en cuanto la investigación sobre aspectos teóricos basada en la tipificación de las conductas fraudulentas, que tratan nuevas figuras punitivas pero que son importantes vincularse en razón de una realidad del desarrollo cibernético.

Alfia (2024) refieren que el crimen de estafa con tarjetas de crédito comprende dos acciones: la sustracción de identidad y el fraude en sí mismo utilizando medios tecnológicos para ejecutar sus acciones. Tres entidades (OJK, Policía y Banco) se esfuerzan por prevenirla.

La legislación penal convencional resulta menos eficaz para estos crímenes, siendo la ley de información y transacciones electrónicas (UU ITE) más adecuada debido al carácter cibernético del fraude abordando tanto la previsión como la persecución de estos delitos, considerando su naturaleza transnacional y altamente técnica.

Farwansyah (2022) detalla como el desarrollo de la tecnología e información es proporcional al desarrollo y crecimiento del crimen de ciberdelito, entre ellos el "Carding" perjudicando a individuos, empresas o instituciones públicas, facilitando datos de índole privada, siendo esto detallado por Titus Reid quien afirma que el cibercrimen abarca "data diddling, the Trojan horse, the salami technique, superzapping, and date leakage", además, se debe ser consciente de que estos delitos se pueden cometer sin reconocer fronteras territoriales y sin interacción directa entre el autor y la víctima del delito.

Caro y Reyna (2023), afirman que la persecución penal se define como un sistema normativo establecida por el Estado, a través de sus instituciones, para sancionar a quienes han cometido conductas punibles. Esto implica la ejecución de la ley penal con el fin de buscar la seguridad jurídica y mantener el orden social quebrantado por la acción delictiva.

El propósito del enjuiciamiento penal es responsabilizar a las personas que participan en actos ilícitos, lo que implica aprehender a esas personas, por ejemplo, a través del debido proceso, y condenarlas cuando sea necesario conforme a la ley.

Por otro lado, Caro y Reyna (2023) afirman que la determinación del castigo es la institución a través de la cual un juez criminal impone una sanción al delincuente por varios factores, como la magnitud del daño, la modalidad en que ocurrió el hecho y otras disposiciones con las que la ley debe estar de acuerdo. No se trata solo de castigar al culpable, sino también de reparar el daño y desalentar el comportamiento desviado.

Finalmente, definen la política criminal como el conjunto de estrategias, normas y medidas diseñadas e implementadas por el estado con el fin de recuperar la validez de la norma afectada por el crimen. La naturaleza de este objetivo se centra tanto en el castigo como en la reforma, estableciendo una base sobre la cual revisar e introducir soluciones para el carding, guiados por estrategias legales y sociales.

El fenómeno del crimen, el castigo y la política criminal, y sus interrelaciones; así podemos estar mejor preparados para promover una tecnología más sofisticada de aplicación humana para enfrentar los desafíos del mundo social emergente (el entorno digital) caracterizado por la complejidad y la incertidumbre. Relacionado con la justificación del problema planteado, se ajusta a la realidad de la sociedad o convivencia de los ciudadanos para tener una buena convivencia (Arias et al., 2022). A pesar de los avances respecto al carding teóricamente y en el derecho, la falta de protección de datos y la confianza pública subyacen a desafíos significativos para abordar y comprender estos fenómenos comunes.

Se ha identificado que, aunque la legislación, como la Ley de Delitos Informáticos en Perú, crea un marco normativo de mínimos, han enfrentado algunas limitaciones de orden práctico, debido a la complejidad y carácter transnacional de los delitos informáticos (Vinelli, 2021). Por otra parte, de acuerdo a Ayyagari (2020) quien presenta investigación sobre cómo la cibernética trata las vicisitudes resultantes de fraudes dentro del contexto del cibercrimen. Aunque conceptualmente la teoría del crimen y la política criminal representa una fuerte base estructural desde la cual se puede realizar el análisis con esperanza, aún queda una brecha conceptual significativa en cuanto a lo que se puede considerar nuevos comportamientos delictivos emergentes en este nuevo entorno digital.

Este estudio se justifica principalmente en términos de la influencia del carding en la confianza social y los derechos básicos de los ciudadanos, con el objetivo de promover y ofrecer diferentes perspectivas para el desarrollo de políticas más efectivas. También sirve a instituciones públicas y privadas al proporcionar herramientas conceptuales y operativas para prevenir, detectar y sancionar estos delitos. Socialmente, favorece la protección de los datos personales.

Carbajal (2021) ha tratado en la investigación la problemática sobre los aspectos de la fiscalía en cuanto las investigaciones que se realizan contra el crimen cibernético, ha sido importante toda vez que existe un progreso acelerado de los actos delincuenciales en diferentes modalidades fraudulentas, y que la fiscalía debe seguir capacitándose en tecnologías avanzadas.

Kaspersky (2024) como una entidad de investigación vinculada con la Interpol en España, se ha realizado actividades de búsqueda y enfrentamiento contra troyanos que vulneran información reservada por lo tanto sigue desarrollando investigación selectiva, para erradicar actos delictivos con la cibernética y el fraude.

Acosta et al. (2020) indican que los crímenes informáticos generan debates importantes debido a su carácter innovador y al continuo cambio de las redes digitales. Estos crímenes revelan la fragilidad de los sistemas de computación, lo que requiere implementar estrategias avanzadas, entre ellas, la puesta en marcha de sistemas informáticos avanzados y la inclusión de inteligencia artificial para identificar y evitar intrusiones.

Dentro del marco de los fraudes informáticos, el estudio de estos crímenes muestra un efecto profundo en la sociedad. Aunque el progreso tecnológico es esencial, Sandoval et al. (2024) enfatizan la importancia de un sólido marco regulatorio, este marco debe asegurar que la innovación tecnológica no ponga en riesgo la seguridad y la privacidad de las personas, logrando un balance entre el avance y la salvaguarda de los derechos esenciales.

Que con respecto de las investigaciones tenemos otras modalidades, como señala Amaquema (2023) se encuentra el phishing, el cual consiste en un fraude cibernético donde delincuentes crean sitios web falsos con el objetivo de engañar a los usuarios y sustraer sus datos bancarios, apropiándose de sus recursos. Este crimen ha crecido con las recientes tendencias digitales, provocando severos perjuicios a la población.

Riega et al. (2021) un tratamiento de los delitos informáticos en sus nuevas modalidades como se siguen desarrollando por el desarrollo de la ciencia en la cibernética, en todo caso es importante poner los hitos dentro de las medidas pertinentes a través del análisis normativo y viendo la situación social real de contemplar el sistema democrática.

Vitteri (2022) trata sobre los aspectos de los delitos informáticos en todo caso busca la implementación de aportes normativos para de esta manera combatir la delincuencia a nivel de la informática con aportes puntuales y asimismo también con medidas preventivas como también aspectos preventivos.

Villarroel y Gutiérrez (2024) resalta aspectos importantes en el tratamiento de la investigación sobre la participación de las entidades de control como debe ser la Superintendencia del Mercado y Valores, en cuestión sobre estos temas, toda vez que está vinculado con la pérdida económica a través de los fraudes cibernéticos que tienen que ser controlados para evitar pérdidas tanto en lo particular y también en razón del Estado.

Velita (2021) examina el rol del fiscal en la investigación previa a juicio, subrayando la relevancia de valorar los recursos de prueba y establecer la idoneidad de los comportamientos delictivos dentro del contexto legal, especialmente en situaciones donde las acciones ilícitas pueden tener una relación con otras relacionadas con lo delictivo.

Rodríguez (2020) identifica a el fraude informático como una problemática dentro del ordenamiento punitivo destacando la responsabilidad administrativa de los representantes de las empresas. Paguay (2020) aborda las tendencias de calzar nuevas conductas delictivas en las eras de la cibernética, resaltando la participación de investigadores y fiscales en su estudio.

Plasencia et al. (2023) investiga sobre como el surgimiento de nuevas formas delictivas, como el phishing y el pharming, han presentado retos extra al sistema penal. Estas modalidades de estafa facilitan a los ciberdelincuentes la adquisición de información personal a través de sitios web falsos o métodos de redireccionamiento malintencionado. Béjar (2023) aborda sobre los aspectos de la organización notarial en cuanto se resuelven los problemas con una debida organización para ello es importante el Compliance, como una medida que siempre se debe aplicar en las instancias notariales respecto de los trámites digitales es importante la protección de la cibernética.

Núñez y Menezes (2020) relacionan la actividad delictiva en el sector administrativo con la corrupción en empresas y organismos estatales. Mayo (2022) destaca que la fiscalía intensifique su combate contra el cibercrimen, incorporando nuevas modalidades como el "pharming", para salvaguardar a los ciudadanos de estafas digitales.

Cárcamo (2023) debate sobre la equiparación de infracciones administrativas con delitos, lo que podría generar conflictos con el principio de última ratio, que prioriza sanciones administrativas sobre penales, reservando las últimas para casos extremos. Herrera et al. (2023) enfatiza en las observaciones del *compliance* del cual la figura principal para prevenir las omisiones que promueven el progreso de la ciberdelincuencia. Respecto a la propiedad y la ciberseguridad, García (2021) aborda temas de propiedad y cautela de la propiedad y alerta acerca de la vulnerabilidad de las transacciones en línea, recomendando así combatir con ellos con normas y tecnología, mientras que Pietrek y Skelnik (2023) resaltan lo esencial de tratar el *carding* desde un enfoque preventivo y social.

Artica (2022) resalta la importancia de definir normas claras en el Poder Judicial, mientras que Estrada (2024) destaca la necesidad de clasificar correctamente los delitos informáticos. Quispe (2021) enfatiza el efecto de la ciberdelincuencia en Mypes, en el sentido de la necesidad de establecer también regulaciones de protección legal de las tecnologías virtuales. Diez (2021) incentiva la colaboración internacional más eficaz para así luchar contra estos crímenes.

En este sentido, se estableció el objetivo general de la investigación siguiente: ¿Determinar en qué medida el carding se relaciona con la protección de datos personales en Lima Metropolitana 2024-2025? Asimismo, el objetivo específico uno precisa lo siguiente: ¿Determinar en qué medida el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados? también en el caso del objetivo específico dos dice: ¿Determinar en qué medida el tráfico de tarjetas de crédito se relaciona con la afectación a las empresas que prestan servicios por internet?

## 2. MÉTODO

### 2.1 Tipo y diseño de investigación

El tipo del trabajo de investigación se ha realizado sobre el estudio básico, la misma que implica ser un trabajo desde un aspecto teórico y por lo tanto también se indica que es fundamental teniendo en cuenta que sirve como aporte fundamento para otros trabajos académicos en el mismo enfoque cuantitativo por el cual se ha desarrollado este trabajo.

Asimismo es puro por el hecho de ser original en cuanto el planteamiento que realiza el investigador en su óptica de la observación del problema planteado; en cuanto al diseño de la investigación se ha tenido en cuenta el no experimental, a razón de no hacer manipulación de variables las mismas que sólo son observadas desde su realidad social para poder aportar con aspectos teóricos de la realidad presentada, pero que si existe la intervención del aspecto estadístico para poder alcanzar resultados originales de la problemática observada, a razón del problema analizado como viene a ser los delitos vinculado con la informática, teniendo modalidades en cuanto la vulneración de los datos personales.

A razón del diseño este se relaciona con la obtención o el acopio de la información la misma que se realiza a través del carácter transversal la que implica extraer información en una sola etapa de la realidad social, en cuanto el personal de apoyo en la investigación puede apersonarse al lugar y poder entregar los instrumentos y con ello poder tener la originalidad y realidad de la extracción de información con el llenado del cuestionario (Setiawan et al., 2022).

En cuanto el trabajo de investigación se ha recolectado la información a personas afectadas con la modalidad del carding como viene a ser el tráfico de tarjetas de crédito, que se ha dado en un periodo de tiempo corto. Asimismo, la investigación es de nivel correlacional también conocida como relacional, por el hecho de verificar la relación de las variables en mención, en este sentido tenemos el siguiente diagrama:

Donde:

M = Es la muestra de la población.

O<sub>1</sub> = Observación de datos personales.

r = Coeficiente de correlación entre variables.

O<sub>2</sub> = Observación de delitos informáticos.

## 2.2 Población, muestra y muestreo

El trabajo de investigación, para efectos de su desarrollo de ejecución del instrumento ha tenido una población de aproximadamente de 500 personas las cuales han sufrido el problema de la pérdida de sus tarjetas de crédito o la respectiva sustracción por delincuentes, claro está en la ciudad de Lima, en todo caso se ha buscado situaciones similares que hayan sufrido por la pérdida de dicho documento. A razón de la muestra, esta ha sido proporción significativa de dicha población indicada, para efectos de que los resultados tengan vinculación relevante con la problemática abordada en este contexto se ha desarrollado mediante un muestreo no probabilístico, el cual se basa en la decisión del investigador para seleccionar y determinar la cantidad de personas que formarán parte de la encuesta correspondiente. En cuanto al muestreo, este proceso se define por el método mediante el cual se decide elegir la muestra, la cual representa a la población de interés. Este procedimiento es lo que se conoce como muestreo.

## 2.3 Hipótesis

### *Hipótesis general*

Hi: Probablemente el carding se relaciona con la protección de datos personales en Lima Metropolitana 2024-2025.

Ho: Probablemente el carding no se relaciona con la protección de datos personales en Lima Metropolitana 2024-2025.

### *Hipótesis específicas*

#### **He1.-**

**Hi.- Probablemente** el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados.

**Ho.- Probablemente** el tráfico de tarjetas de crédito no se relaciona con la pérdida económica de los usuarios afectados.

#### **He2.-**

Hi.- Probablemente el tráfico de tarjetas de crédito se relaciona con la afectación a las empresas que prestan servicios por internet?

Ho.- Probablemente el tráfico de tarjetas de crédito no se relaciona con la afectación a las empresas que prestan servicios por internet.

## 2.4 Variables y operacionalización

**Variable 1:** Carding.

**Variable 2:** Datos personales.

Cuadro de operacionalización de variables se observa en anexo 2.

**2.5 Técnicas e instrumentos de recolección de datos, validez y confiabilidad**

Se ha empleado la técnica de la encuesta, esta situación implica la utilización de un instrumento debidamente validado y por ende para realizar dicha medida de hacer encuesta con la población es necesario la facilitación a través del cuestionario de diez preguntas (ver anexo 5) que viene a ser el instrumento, claro está bajo el cumplimiento de determinados procedimientos, que son aspectos normativos que se establecen para su mejor validez y este punto se ha llevado a cabo con los expertos en la materia penal toda vez que dichas personas han realizado trabajos de investigación y por lo tanto saben de la estructuración debidamente adecuadas en cuestión de las preguntas planteadas y en ese sentido es que los expertos han indicado que dicho instrumento es aplicable para su ejecución en la población ya determinada.

En cuanto la confiabilidad del instrumento aplicado se ha realizado bajo una aplicación del coeficiente alfa de Cronbach, por la cual se establece la consistencia interna, por la obtención de un valor positivo.

**2.6 Procedimientos**

En cuanto al procedimiento primero se ha realizado el objetivo del trabajo de investigación para observar la finalidad y con ello vincularse con la elaboración del instrumento, que seguidamente se ha revisado por los expertos que poseen el grado de Maestro o superior, que han validado el instrumento, seguidamente se ha llevado el trabajo de campo con la entrega del cuestionario a la población indicada que han sido las personas afectadas por los delitos informáticos en especial de la figura del carding, habiendo recibido dicha información se ha tabulado en una hoja de cálculo para finalmente poder ser sometida al programa SPSS.

**2.7 Análisis de datos**

Esta se ha procesado utilizando el programa SPSS, en cuanto la información acopiada producto de que la población ha recibido un cuestionario y además estos han resuelto el mismo por lo que se tiene una data importante, la misma que se ha introducido al programa respectivo y al procesar la información para la obtención del coeficiente de Alfa de Cronbach, en todo caso dicho programa mide el nivel de confiabilidad con razón de las variables en este caso con carding y por otro lado en cuanto los datos personales que han sido altamente positivas.

Que asimismo los análisis de datos también se realizan en relación de la medición del coeficiente de relación de las variables esto en función de la contrastación de hipótesis a través del Rho Spearman, que mide el nivel de correlación en cuanto al trabajo de investigación se resuelto que existe un alto nivel de correlación de las variables en relación de las hipótesis, en todo caso con la hipótesis general el valor de correlación es de 0.93, demostrando altamente su correlación positiva.

## **2.8 Aspectos éticos**

Estos aspectos están vinculados con la aplicación de los instrumentos de investigación, los cuales deben ser implementados de manera correcta y dirigidos a las personas relacionadas con la problemática de estudio. Además, estos principios éticos se han verificado con el fin de garantizar transparencia en el trabajo académico y en el tratamiento de conductas delictivas asociadas a los delitos informáticos. En este contexto, es fundamental considerar el uso de las normas APA, aspecto que suele descuidarse con frecuencia. Cumplir con estas normas implica presentar un trabajo bien estructurado, tanto en su forma como en su estética. Por otro lado, los datos recopilados deben manejarse con reserva, asegurando la confidencialidad durante todo el proceso de investigación.

### 3. RESULTADOS

#### 3.1. Análisis de fiabilidad

**Tabla 1**

*Muestra procesada*

Resumen de procesamiento de casos			
		N	%
Casos	Válido	50	100,0
	Excluido <sup>a</sup>	0	,0
	Total	50	100,0

*Nota. a. La eliminación por lista se basa en todas las variables del procedimiento.*

**Tabla 2**

*Fiabilidad obtenida*

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,907	10

**Interpretación:** Los hallazgos en el análisis de fiabilidad determinaron que el procedimiento consumado para medir las variables, es rotundamente confiable al haberse tenido una cifra de 0,907 afianzando los resultados obtenidos.

**Tabla 3**

*Fiabilidad de cada ítem*

Estadísticas de total de elemento				
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlació n total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
¿Conoce usted la figura del fraude que tiene como denominación el término carding?	11,52	5,683	,822	,887
¿Considera usted que el fraude cibernético perjudica los derechos personales?	11,68	6,875	,497	,908
¿Considera usted que el sistema de compra online es seguro en la comunidad?	11,32	5,447	,753	,894

¿Considera usted que el carding viola los derechos basados en los datos personales de los individuos?	11,62	6,281	,696	,897
¿Considera usted que el fraude cibernético perjudica a las empresas que venden por el sistema online?	11,42	5,391	,849	,885
¿Considera que la existencia de un mercado negro de compra de tarjetas robadas es la causa del carding?	11,48	5,520	,850	,885
¿Considera usted que la consecuencia del fraude a nivel de suplantar datos en las tarjetas de crédito perjudica al titular de ella?	11,64	6,439	,659	,900
¿Considera usted que el carding tiene consecuencias en las empresas financieras?	11,36	5,378	,808	,889
¿Considera usted que es importante monitorear las tarjetas de cuentas bancarias regularmente para la protección de los datos personales?	11,66	6,637	,595	,903
¿Considera usted que las tarjetas virtuales son importantes para evitar las conductas fraudulentas del carding?	10,78	7,155	,170	,919

**Tabla 4***Estadística del ítem N° 1*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
	Si	40	80,0	80,0	80,0
Válido	No	10	20,0	20,0	100,0

Total	50	100,0	100,0
-------	----	-------	-------

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 80,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 20,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 5**

*Estadística del ítem N° 2*

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	48	96,0	96,0
	No	2	4,0	100,0
	Total	50	100,0	100,0

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 96,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 4,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 6**

*Estadística del ítem N° 3*

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	30	60,0	60,0
	No	20	40,0	100,0
	Total	50	100,0	100,0

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 60,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 40,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 7**

*Estadística del ítem N° 4*

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
	Si	45	90,0	90,0

Válido	No	5	10,0	10,0	100,0
	Total	50	100,0	100,0	

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 90,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 10,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 8**

*Estadística del ítem N° 5*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
	Si	35	70,0	70,0	70,0
Válido	No	15	30,0	30,0	100,0
	Total	50	100,0	100,0	

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 70,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 30,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 9**

*Estadística del ítem N° 6*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
	Si	38	76,0	76,0	76,0
Válido	No	12	24,0	24,0	100,0
	Total	50	100,0	100,0	

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 76,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 24,0% optó por afianzar la opción “No”.

**Tabla 10**

*Estadística del ítem N° 7*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
	Si	46	92,0	92,0	92,0

Válido	No	4	8,0	8,0	100,0
	Total	50	100,0	100,0	

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 92,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 8,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 11**

*Estadística del ítem N° 8*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	32	64,0	64,0	64,0
	No	18	36,0	36,0	100,0
	Total	50	100,0	100,0	

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 64,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 36,0% optó por afianzar la opción “No”.

**Tabla 12**

*Estadística del ítem N° 9*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	47	94,0	94,0	94,0
	No	3	6,0	6,0	100,0
	Total	50	100,0	100,0	

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 94,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 6,0% optó por afianzar la opción “No”.

**Tabla 13**

*Estadística del ítem N° 10*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	3	6,0	6,0	6,0
	No	47	94,0	94,0	100,0

Total	50	100,0	100,0
-------	----	-------	-------

**Interpretación:** Los hallazgos de la sumatoria del presente ítem, han precisado que un 6,0% contemplo en afianzar la opción “Si”, en el mismo momento se estableció que un 94,0% optó por afianzar la opción “No”, esto en cuanto al total de encuestados.

**Tabla 14**

*Rangos estadísticos que esclarecen el contraste de la hipótesis general*

Correlaciones para contrastar las hipótesis				
			V1	V2
Rho de Spearman	V1	Correlación-Rango	1,000	0,923**
		Sig. (bilateral)	.	0,000
		N	50	50
	V2	Correlación-Rango	0,923**	1,000
		Sig. (bilateral)	0,000	.
		N	50	50

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

**Interpretación:** Los hallazgos han esclarecido que la cifra en la correlación fue de 0,923, confirmando que las variables están correlacionadas, ante todo porque la Sig. (bilateral) fue de 0,000 y a la vez fue inferior a 0,05. Es perceptible entonces determinar el rechazo de la hipótesis nula.

**Tabla 15**

*Rangos estadísticos que esclarecen el contraste de la hipótesis específica 1*

Correlaciones para contrastar las hipótesis				
			Variable 1	Variable 2
			Dimensión 1	Dimensión 1
Rho de Spearman	Variable 1 Dimensión 1	Correlación-Rango	1,000	0,890**
		Sig. (bilateral)	.	0,000
		N	50	50
	Variable 2 Dimensión 1	Correlación-Rango	0,890**	1,000
		Sig. (bilateral)	0,000	.
		N	50	50

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

**Interpretación:** Los hallazgos han esclarecido que la cifra en la correlación fue de 0,890, confirmando que las dimensiones están correlacionadas, ante todo porque

la Sig. (bilateral) fue de 0,000 y a la vez fue inferior a 0,05. Es perceptible entonces determinar el rechazo de la hipótesis nula.

**Tabla 16**

*Rangos estadísticos que esclarecen el contraste de la hipótesis específica 2*

Correlaciones para contrastar las hipótesis				
			Variable 1	Variable 2
			Dimensión 2	Dimensión 2
Rho de Spearman	Variable 1	Correlación-Rango	1,000	0,758**
		Sig. (bilateral)	.	0,000
	Dimensión 2	N	50	50
		Correlación-Rango	0,758**	1,000
	Variable 2	Sig. (bilateral)	0,000	.
		Dimensión 2	N	50

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

**Interpretación:** Los hallazgos han esclarecido que la cifra en la correlación fue de 0,758, confirmando que las dimensiones están correlacionadas, ante todo porque la Sig. (bilateral) fue de 0,000 y a la vez fue inferior a 0,05. Es perceptible entonces determinar el rechazo de la hipótesis nula.

#### 4. DISCUSIÓN

**Primera discusión.** - En cuanto los resultados, debidamente establecidos es necesario discutirlos con los antecedentes que son estudios previos realizados de acuerdo a las variables del trabajo de investigación, así como también las teorías que se han utilizado referente al informe final; en cuestión de la hipótesis general se encontró un coeficiente de correlación de 0.923; indicando una relación positiva muy fuerte entre las variables de carding y datos personales, con una significancia bilateral  $< \alpha 0.05$ ; por lo tanto se excluye la hipótesis nula y se acepta la hipótesis inicial.

**Segunda discusión.** - En cuestión de los hallazgos que implican los resultados del trabajo de investigación van en todo caso a confirmar lo indicado por Fennelly y Perry (2020). que trata sobre los aspectos para la protección de datos en cuanto la problemática de los delitos informáticos en estas circunstancias hay que tener en cuenta dicha situación ya que el Alfa de Crombach, mide el nivel del valor de fiabilidad de las variables; siendo así se ha determinado en una conclusión que existe una alta relación positiva entre el carding y la protección de los datos personales toda vez que ante el aumento del carding como una medida contraria a la ley en cuestión que estamos hablando de un fraude cibernético en la utilización de las tarjetas de crédito para extraer dinero de manera ilícita; en este sentido se ha determinado una alta relación directa puesto que cuando hay mayor carding como la obtención e utilización para el mal de tarjetas de crédito, es importante que ante el aumento de este tipo de fraude, por consiguiente también se incrementa la protección de datos personales, asimismo todo lo indicado también se relaciona con Alcalá y Meléndez (2023) en cuanto dichos autores también establecen la problemática de los delitos financieros como un problema social, de relevancia jurídica en cuanto a los fraudes cibernéticos.

**Tercera discusión.** - En cuanto a la hipótesis específica, que señala probablemente el tráfico de las tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados; con los resultados se ha establecido la aceptación de la referida hipótesis, y por ende rechazar la hipótesis nula en cuanto niega esta probabilidad; siendo así es que en la sociedad en la actualidad existe el tráfico de tarjetas de crédito lo que se realiza a los especialistas en cibernética con la cual pueden conseguir virtualmente datos personales y con ello generar compras online y por otro lado extraer dinero de otra persona, en esta situación se vincula con una relación directa por que esta afectación genera en el titular del documento la pérdida de su capital generan un perjuicio económico; en este sentido estos

resultados se relación con Zambrano (2022) por la cual dichos autores informan sobre la situación de las pérdidas económicas de los usuarios en cuanto esta situación delincinencial y más aún no solamente contra el usuario sino que también afecta la economía de las empresas donde se extrae el dinero falseando datos personales, generando de esta manera otra problemática toda vez que cuando se hace el reclamo el banco no tiene los aspectos de protección de sus tarjetas digitales y muchas veces son tardía sus reacciones quedando en un perjuicio del usuario afectado.

**Cuarta discusión.** - En cuanto a la hipótesis específica dos que señala probablemente el tráfico de las tarjetas de crédito se relaciona con la afectación a las empresas que coadyuvan en el servicio por internet; que producto de los hallazgos se ha podido determinar que se ha establecido una alta relación positiva de las variables en mención por lo cual se acepta que existe relación del tráfico de tarjetas de crédito con la afectación de las empresas que prestan servicios de internet; y por ende al tener el  $p < 0.05$  es que se rechaza la hipótesis nula; en todo caso su correlación es de 0.758 siendo positiva la correlación.

Toda esta situación se vincula con Peña (2023) y Carriedo (2022) que tratan la situación de la vulneración de los derechos de los usuarios y asimismo de las empresas que trabajan mediante el servicio de internet, que se han visto vulnerados en sus ingresos económicos por la situación de la utilización de dichas tarjetas para una realización de pagos en partes de lo cual sólo se paga la primera parte y lo demás ya no se paga perdiendo su capital dichas empresas; en todo caso toda esta situación se ve también en perjuicio del usuario que ha sido afectado en sus datos personales y que estas se ven vulneradas por estos actos que lindan con lo delictivo. Asimismo, esta situación ha provocado todo un impacto en el sistema financiero producto de estos actos delictivos en cuanto la suplantación vía teléfono por lo que se genera una doble afectación tanto para el usuario como también para la entidad bancaria, y que por lo demás no está cumpliéndose las medidas de seguridad que siempre llegan en forma tardía cuando ya se ha generado el acto delictivo y la afectación a los mencionados (Saryo et al., 2023).

En todo caso esta hipótesis aceptada también se relaciona con Carriedo (2022) en cuanto dicho trabajo de investigación a nivel internacional como es en México se ha visto resaltar la violación de los derechos de las personas en cuanto un bien jurídico se protege como es el patrimonio es así que se está vulnerando un derecho fundamental del individuo, por lo que se debe tipificar estos hechos dentro de los

ordenamientos punitivos de los Estados. Asimismo Trucios (2023) ha realizado un trabajo de investigación con vinculación de los hallazgos en razón de la utilización de menores pero de manera virtual y como de esta manera se vulnera la situación de los menores en acciones delictivas en la virtualidad y por ende son actos calificados como infracciones a la ley penal, pero que esta situación lo llevan a más cuando son los menores utilizados para la explotación laboral y muchas veces las menores en la explotación sexual es por ello que el trabajo es importante por el hecho de que se deben adoptar medidas públicas en cuanto las normas de sanción como políticas de Estado.

En todo caso la problemática también se vincula con los hallazgos a razón de Ocupa (2022) en razón de los convenios que se han realizados de manera internacional y al cual el Perú es parte en todo caso tenemos el Convenio de Budapest para la cual es importante fortalecer las estrategias contra estos actos delictivos de la ciberdelincuencia y como con todos estos antecedentes se puede tipificar y sancionar jurídicamente la situación del carding con lo que se va a garantizar la seguridad digital y por último tenemos a Sotomayor (2022) trabajo de investigación importante para efectos de hacer un buen tratamiento de estas conductas delictivas, por el hecho de que no se califica adecuadamente estos hechos dentro del proceso, por lo que la defensa desnaturaliza dichas conductas delictivas en falta de los medios probatorias para poder calificar dichas conductas y por consiguiente no se puede establecer una adecuada sanción punitiva.

## 5. CONCLUSIONES

**Primero:** Que se ha determinado que la relación positiva es muy fuerte entre las variables de la hipótesis general las cuales son el carding y la protección de datos personales; debido a que se halló un  $r=0.923$  y  $p=0.000$ ; estableciendo que, a mayores actos fraudulentos de utilización de datos personales en tarjetas de crédito, es mayor la protección de los datos personales de las personas, que deben implantar las instituciones.

**Segundo:** Que se ha determinado que la relación positiva es muy fuerte entre las variables de la hipótesis específica uno las cuales son el tráfico de tarjetas de crédito y la pérdida de economía de usuarios; debido a que se halló un  $r=0.890$  y  $p=0.000$ ; estableciéndose que a mayor tráfico de tarjetas de crédito es mayor las pérdidas económicas de los usuarios; por lo que se sigue incrementando los fraudes de las tarjetas de crédito y las pérdidas a los usuarios son enormes.

**Tercero:** Se establece que la relación positiva es fuerte entre las variables de la hipótesis específica dos las cuales son el tráfico de tarjetas de crédito y la afectación a empresas online; debido a que se halló un  $r=0.758$  y  $p=0.000$ ; estableciéndose que a mayor tráfico de tarjetas de crédito es mayor la afectación a las empresas de ventas online; por lo que se evidencia el problema del fraude y las pérdidas económicas de las empresas que venden en esta modalidad.

## 6. RECOMENDACIONES

**Primera:** Debe establecerse un proyecto de ley para poder especificar estas nuevas conductas delictivas que nacen con el desarrollo de la actividad cibernética y el desarrollo virtual.

**Segunda:** Que se establezcan medidas protocolares tanto en las instituciones bancarias para efectos de prevenir los fraudes en actividades comerciales por parte de los sujetos que comercializan y utilizan las tarjetas de crédito.

**Tercera:** Que se establezcan medidas protocolares en las empresas que venden por online y con lo cual no tengan pérdidas por las compras fraudulentas y se perjudique al verdadero usuario.

## REFERENCIAS

- Acosta, G., Mendoza, L., & Zamora, P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana De Gerencia*, 17(21), 351-368. <https://doi.org/10.37960/revista.v25i89.31534>
- Alcalá, M., & Meléndez, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. PAAKAT: *Revista de Tecnología y Sociedad*, 13(24), 1–37. <https://dialnet.unirioja.es/servlet/articulo?codigo=8956682>
- Alfia, R. (2024). *Urpaya pencegahan terhadap tindak pidana pencurian kartu kredit (credit card fraud) dalam hukum pidana* [Tesis de pregrado, Universitas Muhammadiyah Malang]. Repository of Universitas Muhammadiyah Malang. <https://eprints.umm.ac.id/id/eprint/10058/>
- Álvarez, C. (2023, 13 de enero). Colombia registró un crecimiento de ataques informáticos en el último año. Voz de América. VOA. *Diario Tecnología*. <https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticosultimoano/6916577.html#:~:text=Colombia%20registr%C3%B3%20en%202022%20m%C3%A1s,computadoras%2C%20tablets%20y%20tel%C3%A9fonos%20celulares>
- Amaiquema, E. (2023). *Análisis del ataque del modelo Phishing en los sistemas informáticos y bancarios* [Tesis de pregrado, Universidad Técnica de Babahoyo]. Repositorio de la Universidad Técnica de Babahoyo. <http://dspace.utb.edu.ec/handle/49000/14773>
- Arévalo, M., & Vega, J. (2022). *Ciberdelitos: Análisis del sistema penal*. Editorial Iustitia. <https://www.juristaeditores.com/producto/ciberdelitos-analisis-en-el-sistema-penal/>
- Arias, J., Holgado, J., Tafur, T., & Vasquez, M. (2022). *Metodología de la investigación: El método ARIAS para desarrollar un proyecto de tesis*. Editorial Instituto Universitario de Innovación Ciencia y Tecnología. <https://doi.org/10.35622/inudi.b.016>
- Artica, A. (2022). *Aplicación de la responsabilidad de naturaleza penal de la persona jurídica a partir de la Ley N°30424 en el Poder Judicial de Lima Norte*. [Tesis de pregrado, Universidad Ricardo Palma]. Repositorio de la Universidad Ricardo Palma. <https://hdl.handle.net/20.500.14138/5831>

- Ayyagari, R. (2020). Data breaches and carding. *Revista The Palgrave handbook of international cybercrime and cyberdeviance*, 12(14), 939–959. [https://doi.org/10.1007/978-3-319-78440-3\\_37](https://doi.org/10.1007/978-3-319-78440-3_37)
- Barahona, V. (2023). *La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima Norte 2022* [Tesis de pregrado, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. <https://hdl.handle.net/20.500.12692/134504>
- Béjar, G. (2023). *Compliance organizacional: Propuesta de una metodología sistémica; caso de aplicación al sector notarial del estado de Nayarit* [Tesis de maestría, Universidad Autónoma de Sinaloa]. Repositorio de la Universidad Autónoma de Sinaloa. [https://www.researchgate.net/publication/374583791\\_Compliance\\_organizational\\_Propuesta\\_de\\_una\\_metodologia\\_sistemica](https://www.researchgate.net/publication/374583791_Compliance_organizational_Propuesta_de_una_metodologia_sistemica)
- Carbajal, M. (2021). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen* [Tesis de maestría, Universidad San Martín de Porres]. Repositorio de la Universidad San Martín de Porres. <https://repositorio.usmp.edu.pe/>
- Cárcamo, A. (2023). La frontera entre el delito penal y la infracción administrativa: una delimitación discrecional entregada a la política legislativa. *Ius et Praxis*, 29(1), 66-85. <https://dx.doi.org/10.4067/S0718-00122023000100066>
- Caro, D., & Reyna, L. (2023). *Derecho Penal: Parte General*. Editorial LP Pasión por el derecho. <https://es.scribd.com/document/677504677/2023-Dino-Caro-Coria-Luis-Reyna-Alfaro-Derecho-Penal-Parte-General>
- Carriedo, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México* [Tesis de maestría, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación]. Repositorio del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. <http://infotec.repositorioinstitucional.mx/jspui/handle/1027/518>
- Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del Estado*. Defensoría Gobierno. <https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf>

- Diez, J. (2021). La Política criminal en las ciencias penales: un análisis crítico de la contribución de Roxin. *Revista Electrónica de Ciencia Penal y Criminología*, 23(02), 1-32. <http://criminet.ugr.es/recpc/23/recpc23-02.pdf>
- El peruano. (2023). *¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú.* El peruano noticias. <https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru#:~:text=21%2F06%2F2023%20Cada%20mes,de%20la%20mitad%20de%20total>
- Estrada, C. (2024). La impunidad en los delitos informáticos: Una problemática de poco interés para legisladores, jueces y fiscales. *Revista Ius Vocatio*, 7(9), 1-25. <https://revistas.pj.gob.pe/revista/index.php/iusVocatio/article/download/928/1261/>
- Farwansyah, A. (2022). *Penegakan Hukum Tindak Pidana Pencurian Data Kartu Kredit (CARDING) Di Wilayah Hukum Kepolisian Daerah Riau* [Tesis de pregrado, Universitas Islam Riau]. Repository of Universitas Islam Riau. <https://repository.uir.ac.id/15332/>
- Fennelly, L., & Perry, M. (2020). Assessing Risk and Vulnerabilities. *Journal Physical Security: 150 Things You Should Know* 11(12), 19-26. [https://doi.org/10.1007/978-3-319-78440-3\\_37](https://doi.org/10.1007/978-3-319-78440-3_37)
- Gaimari, G. (2021). *Inteligencia artificial e impacto en el cibercrimen* [Tesis de pregrado, Universidad de Belgrano]. Repositorio Universidad de Belgrano, Buenos Aires, Argentina. <https://repositorio.ub.edu.ar/handle/123456789/9333>
- García, A. (2021). *Seguridad jurídica y el sistema de transferencia de la propiedad inmueble* [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú. <https://hdl.handle.net/20.500.13067/1145>
- Hatta, A. (2022). *Pertanggungjawaban Pidana Oleh Bank Terhadap Tindak Pidana Penggunaan Kartu Kredit Tanpa Hak (Carding)* [Tesis de maestría, Universitas Islam Riau]. Repository of Universitas Islam Riau. <https://repository.uir.ac.id/13525/>
- Herrera, E., Barrera, K., & Rodríguez, I. (2023). Responsabilidad penal de las personas jurídicas en Perú: una reevaluación del aforismo *societas delinquere nec punire potest* a partir de una perspectiva anticonceptualista. *Revista Direito GV*, 19(23), 1-26. <http://surl.li/wqbchc>

- Kaspersky. (2024). España, uno de los principales objetivos del troyano bancario Grandoreiro. *Kaspersky*. <https://www.kaspersky.es/about/press-releases/espana-uno-de-los-principales-objetivos-del-troyano-bancario-grandoreiro>
- Mayo, C. (2022). *Análisis y técnicas de prevención, detección y ataques de phishing* [Tesis de maestría, Universidad Nacional de Educación a Distancia de España]. Repositorio de la Universidad Nacional de Educación a Distancia de España. <http://surl.li/gbugcl>
- Ninasivincha, M., & Gutiérrez, E. (2023). *Inadecuada gestión de información para reducir la alta incidencia de delitos contra el patrimonio en los Departamentos de Investigación Criminal de Lima* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio de la Pontificia Universidad Católica del Perú. <https://tesis.pucp.edu.pe/repositorio/>
- Nuñez, P., & Menezes, T. (2020) La responsabilidad administrativa de las personas jurídicas desde la perspectiva de la Ley contra la corrupción. *Revista Derecho y Cambio Social*, 59(60), 1-24. <https://dialnet.unirioja.es/servlet/articulo?codigo=7219646&info=resumen>
- Ocupa, B. (2022). *Aplicación del convenio Budapest y delitos informáticos en el Perú, 2022* [Tesis de maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. <https://hdl.handle.net/20.500.12692/119930>
- Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet* [Tesis de pregrado, Universidad Nacional de Chimborazo]. Repositorio de la Universidad Nacional de Chimborazo. <http://dspace.unach.edu.ec/handle/51000/7607>
- Peña, M. (2023). *Delitos Cibernéticos* [Tesis de maestría, Universidad Libre de Colombia]. Repositorio de la Universidad Libre de Colombia. <https://hdl.handle.net/10901/24774>
- Pietrek, G., & Skelnik, K. (2023). Cybersecurity and the scope of designing information security systems in the organization. *Journal Of Modern Science*, 51(2), 141-173. <https://doi.org/10.13166/jms/166583>
- Plasencia, J., Bajo, A., Marrero, F., & Nicado, M. (2023). Gestión de Riesgos de Cumplimiento con Enfoque en Valores Compartidos: Aplicación en un Caso de Estudio en Cuba. *Revista Científica "Visión de Futuro"*, 27(2), 25-41. <https://doi.org/10.36995/j.visiondefuturo.2023.27.02.001.en>

- Quispe, L. G. (2021). *La autorregulación del compliance en la cultura corporativa de las Pymes peruanas* [Tesis de pregrado, Universidad Privada del Norte]. Repositorio de la Universidad Privada del Norte. <https://hdl.handle.net/11537/28658>
- Riega, Y., Huamani, H., & Machuca, J. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Revista Lex*, 19(28), 197-236. <https://dialnet.unirioja.es/servlet/articulo?codigo=8255000>
- Rodríguez, J. (2020). *Una aproximación al delito de estafa en sus modalidades clásica e informática: De la estafa tradicional a las nuevas modalidades como el Phishing* [Tesis de maestría, Universidad de Coruña]. Repositorio de la Universidad de Coruña. <http://surl.li/ywetdt>
- Sagala, S., Esther, J., & Sinaga, J. (2025). Legal Analysis of the Handling of M-Banking Electronic Evidence in Bribery Cases in the Digital Era. *Indonesian Journal of Law and Justice*, 2(3), 1-8. <https://doi.org/10.47134/ijj.v2i3.3625>
- Sánchez, D. (2020). *Estudio teleológico del Carding y BINS. Su impunidad e impacto en el sistema bancario mexicano* [Tesis de pregrado, Benemérita Universidad Autónoma de Puebla]. Repositorio de la Benemérita Universidad Autónoma de Puebla. <https://hdl.handle.net/20.500.12371/11702>
- Sandoval, M., De Almeida, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. *Crime Science*, 13(41), 13-41. <https://doi.org/10.1186/s40163-024-00239-1>
- Saryo, S., Uwiyono, A., & Nurbaiti, S. (2023). Reconstuction of Legal Protection Regulation for Service Customers of Payment System in Indonesia. *UNES Law Review*, 6(2), 5546-5561. <https://doi.org/10.31933/unesrev.v6i2.1358>
- Sauer, W. (2024). *Derecho penal: parte general*. Ediciones Olejnik.
- Setiawan, M. N., Safitri, M., & Lestari, L. (2022). Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia. *Datin Law Jurnal*, 3(2), 633-646. <https://www.ojs.umb-bungo.ac.id/index.php/DATIN/article/view/931>
- Sotomayor, G. (2022). *La calificación fiscal en los delitos informáticos en el distrito fiscal de Lima Centro, 2019 – 2020* [Tesis de maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. <https://hdl.handle.net/20.500.12692/95834>
- Trucios, A. (2023). *La ciberdelincuencia y la captación en menores de edad Lima Metropolitana, 2021* [Tesis de pregrado, Universidad Autónoma del Perú].

- Repositorio de la Universidad Autónoma del Perú.  
<https://hdl.handle.net/20.500.13067/2704>
- Velita, A. (2021). *Problemas de la valoración fiscal en la etapa de investigación preliminar de los delitos de fraude informático en Lima* [Tesis de maestría, Universidad San Martín de Porres]. Repositorio de la Universidad San Martín de Porres. <https://repositorio.usmp.edu.pe/>
- Villarroel, E. G., & Gutiérrez, J. (2024). Dynamic malware analysis using detection algorithms based on machine learning. *Interfaces*, 10(19), 119-138. <https://doi.org/10.26439/interfases2024.n19.7097>
- Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis*, 53(053), 95-110. <https://doi.org/10.26439/iusetpraxis2021.n053.4995>
- Vitteri, G. (2022). *Mecanismos jurídicos para implementar la Ley 30096 en los delitos informáticos contra el patrimonio frente a las nuevas tecnologías informáticas* [Tesis de maestría, Universidad Inca Garcilaso de la Vega]. Repositorio de la Universidad Inca Garcilaso de la Vega. <https://roar.eprints.org/15208/>
- Zambrano, A. (2022). *El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa* [Tesis de maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo\\_V\\_A.pdf](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_V_A.pdf)

## ANEXOS

### Anexo 1. Matriz de consistencia

Título: Las consecuencias del carding en la protección de datos personales lima metropolitana 2024

Problema general	Objetivo general	Hipótesis general	Variables y dimensiones	Metodología
<p>¿En qué medida el carding se relaciona con la protección de datos personales en Lima Metropolitana 2024?</p>	<p>Determinar en qué medida el carding se relaciona con la protección de datos personales en Lima Metropolitana 2024.</p>	<p><b>Probablemente</b> el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados.</p>	<p>V1: carding</p> <p><b>Dimensiones:</b></p> <ul style="list-style-type: none"> <li>• fraude</li> <li>• Estafa</li> </ul>	<p><b>Enfoque:</b></p> <p>Cuantitativo</p> <p><b>Diseño:</b></p> <p>No experimenta</p> <p><b>Nivel:</b></p> <p>Correlacional</p> <p><b>Instrumento:</b></p> <p>Cuestionario</p> <p><b>Unidad de análisis:</b></p> <p>Personas afectadas por el carding</p> <p><b>Muestra:</b></p> <p>50 usuarios</p>
<b>Problemas específicos</b>	<b>Objetivos específicos</b>	<b>Hipótesis específicas</b>		
<p>¿En qué medida el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados?</p>	<p>Determinar en qué medida el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados</p>	<p><b>Probablemente</b> el tráfico de tarjetas de crédito se relaciona con la pérdida económica de los usuarios afectados.</p>	<p>V2: Datos personales</p> <p><b>Dimensiones:</b></p> <ul style="list-style-type: none"> <li>• Derechos fundamentales                             <ul style="list-style-type: none"> <li>• Principios</li> <li>• Doctrina</li> </ul> </li> </ul>	
<p>¿En qué medida el tráfico de tarjetas de crédito se relaciona con la afectación a las empresas que prestan servicios por internet?</p>	<p>Determinar en qué medida el tráfico de tarjetas de crédito se relaciona con la afectación a las empresas que prestan servicios por internet.</p>	<p>Probablemente el tráfico de tarjetas de crédito se relaciona con la afectación a las empresas que prestan servicios por internet</p>		

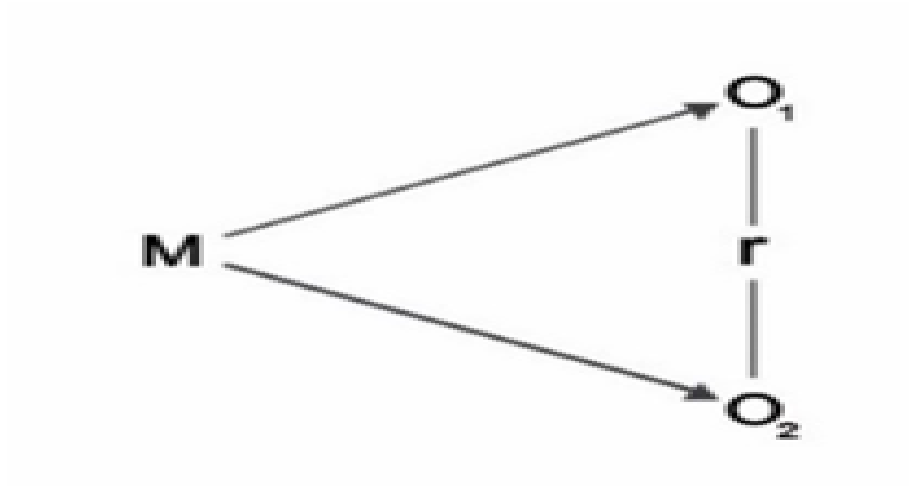
## Anexo 2. Matriz de operacionalización

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición	Instrumento
Carding	Trafico de tarjetas de créditos, como el fraude en el uso indebido	Las variables tanto carding y datos personales se miden por medio de dimensiones en la ejecución del cuestionario que viene a ser un instrumento para la escala de tipo liker	fraude	Engaño Estafa Pérdida económica Uso indebido Compra ilegal Agravio personal Constitución Principios Doctrina Daño personal	Nominal	Cuestionario
Datos personales	Violación de los datos personales como son las generales de ley		Derechos fundamentales			

### Anexo 3. Evidencias de figuras de la aplicación

**Figura 1**

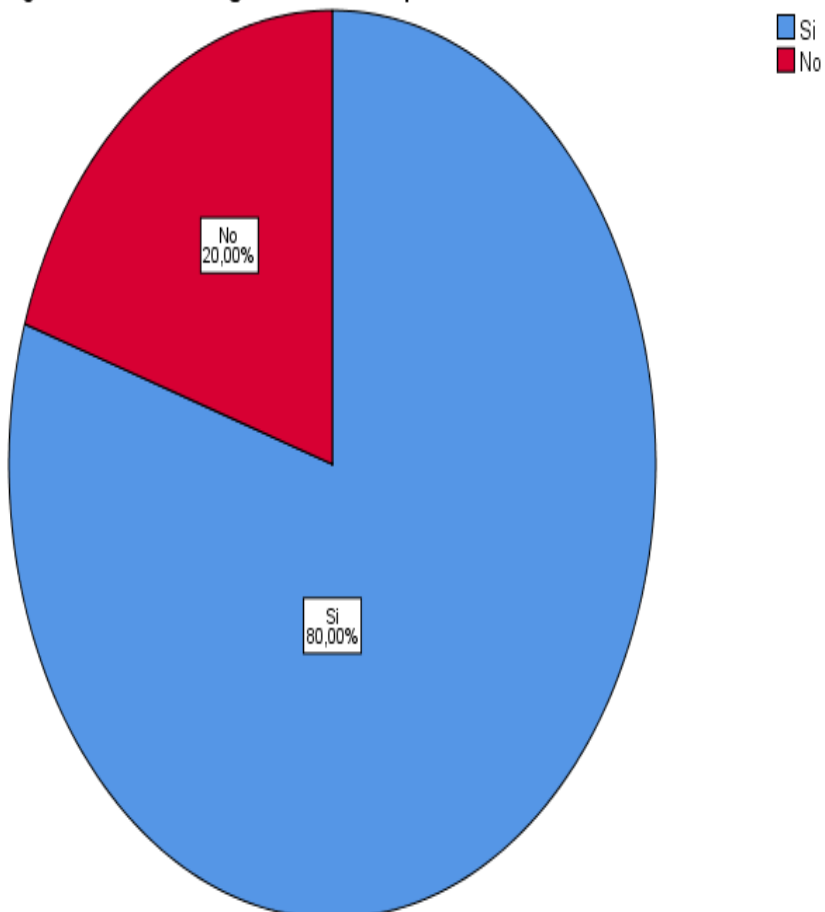
*Diagrama de correlación*



**Figura 2**

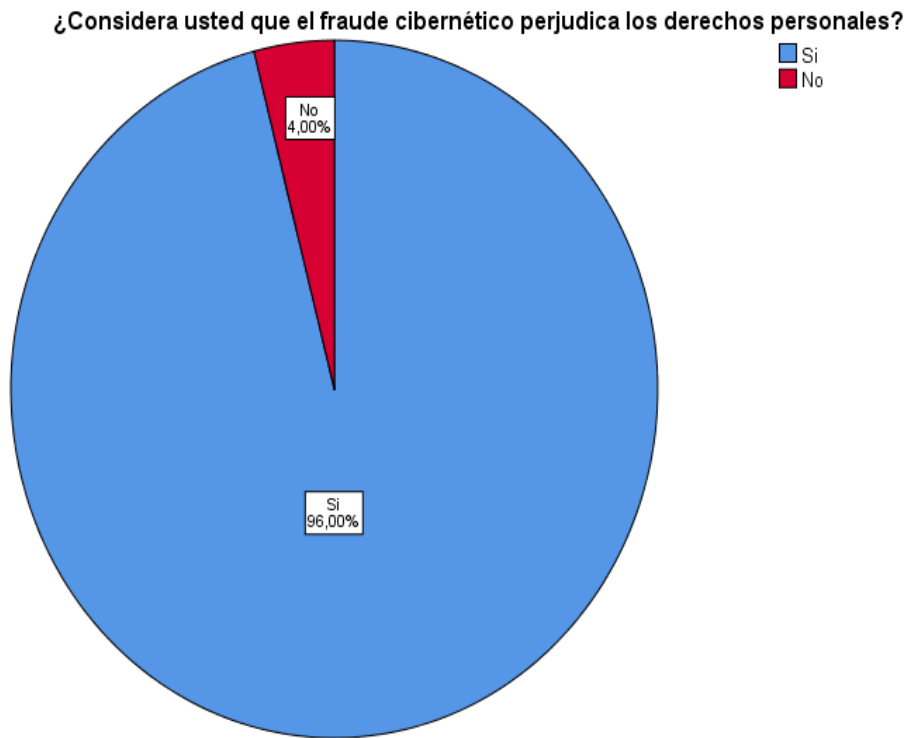
*Resultados de interpretación del ítem N° 1*

¿Conoce usted la figura del fraude que tiene como denominación el término carding?



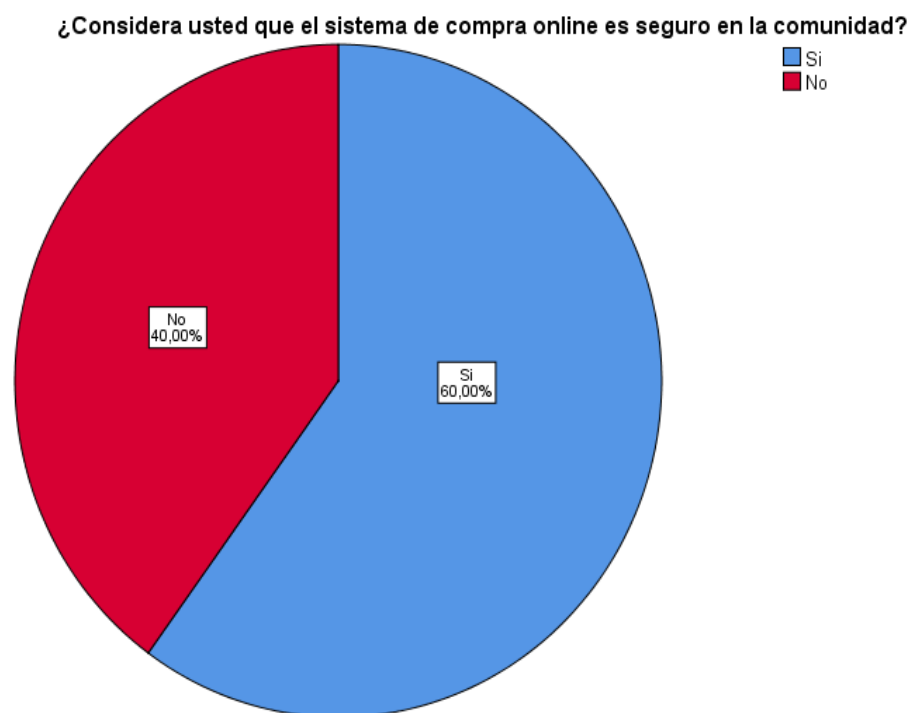
**Figura 3**

*Resultados de interpretación del ítem N° 2*



**Figura 4**

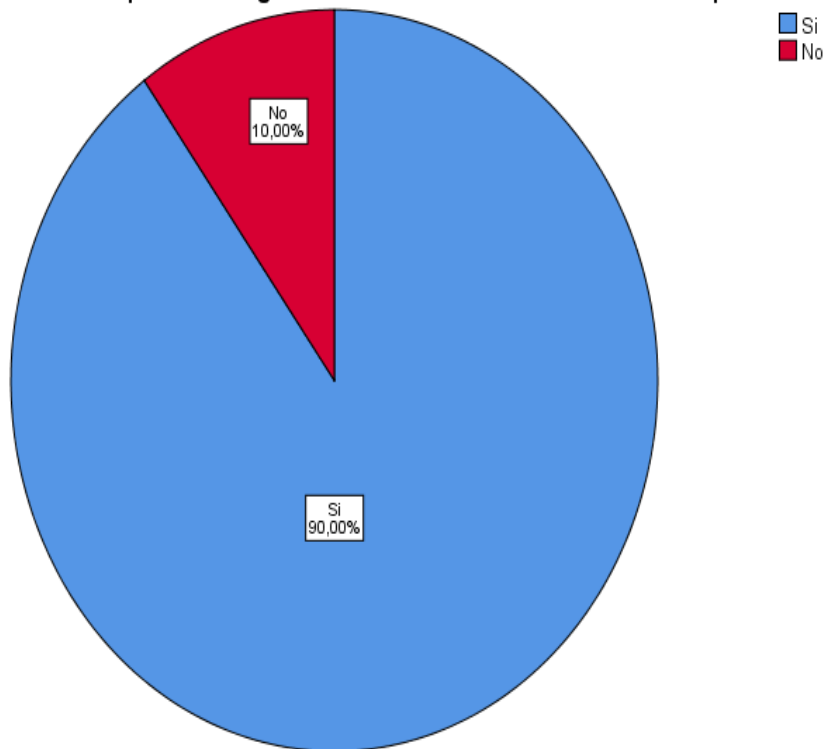
*Resultados de interpretación del ítem N° 3*



**Figura 5**

*Resultados de interpretación del ítem N° 4*

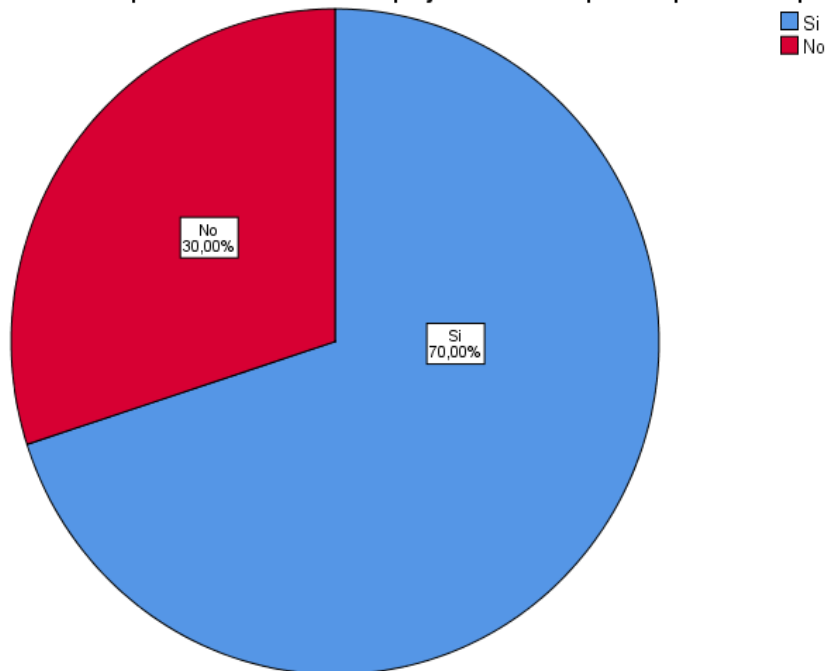
¿Considera usted que el carding viola los derechos basados en los datos personales de los individuos?



**Figura 6**

*Resultados de interpretación del ítem N° 5*

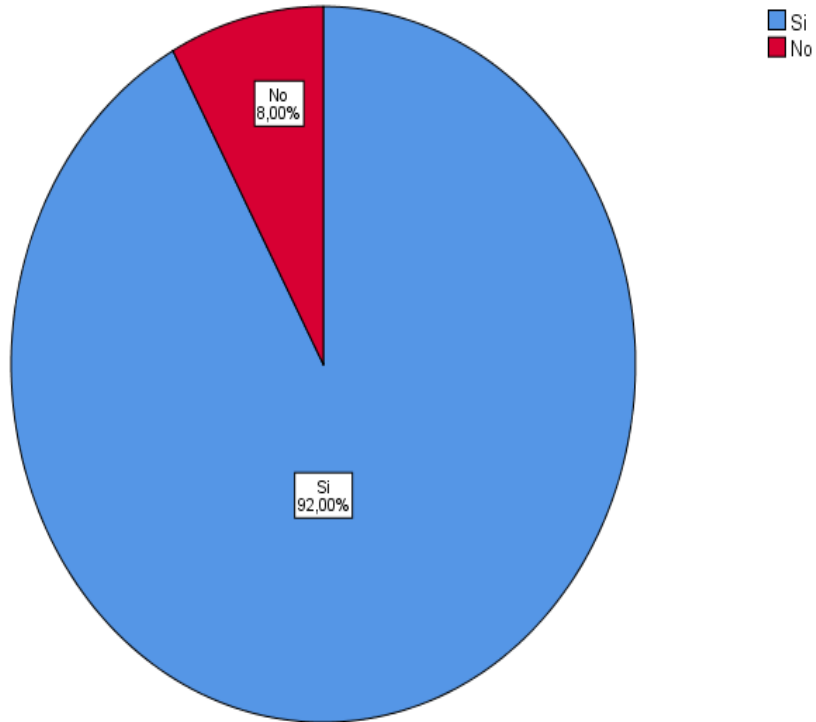
¿Considera usted que el fraude cibernético perjudica a las empresas que venden por el sistema online?



### Figura 7

Resultados de interpretación del ítem N° 6

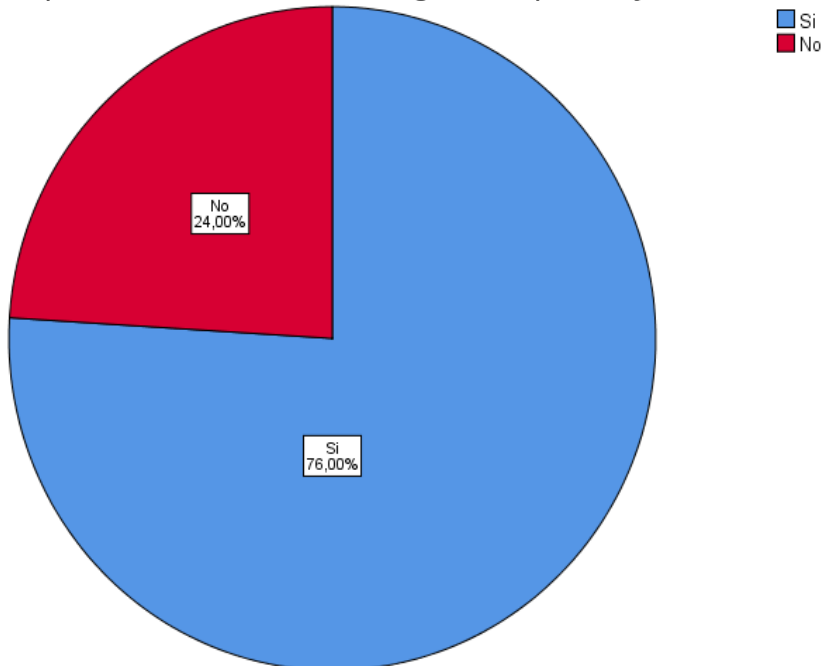
¿Considera usted que la consecuencia del fraude a nivel de suplantar datos en las tarjetas de crédito perjudica al titular de ella?



### Figura 8

Resultados de interpretación del ítem N° 7

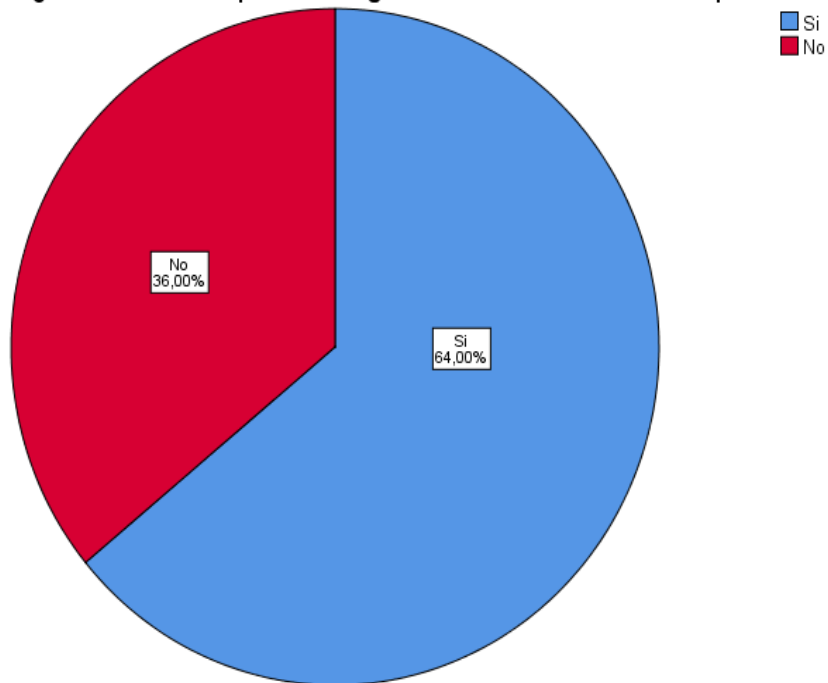
¿Considera que la existencia de un mercado negro de compra de tarjetas robadas es la causa del carding?



**Figura 9**

*Resultados de interpretación del ítem N° 8*

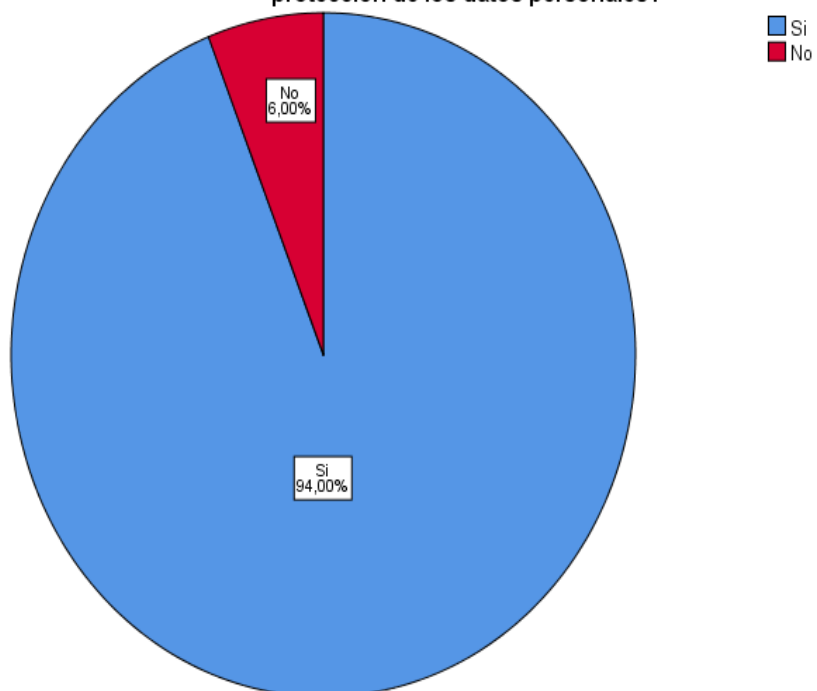
¿Considera usted que el carding tiene consecuencias en las empresas financieras?



**Figura 10**

*Resultados de interpretación del ítem N° 9*

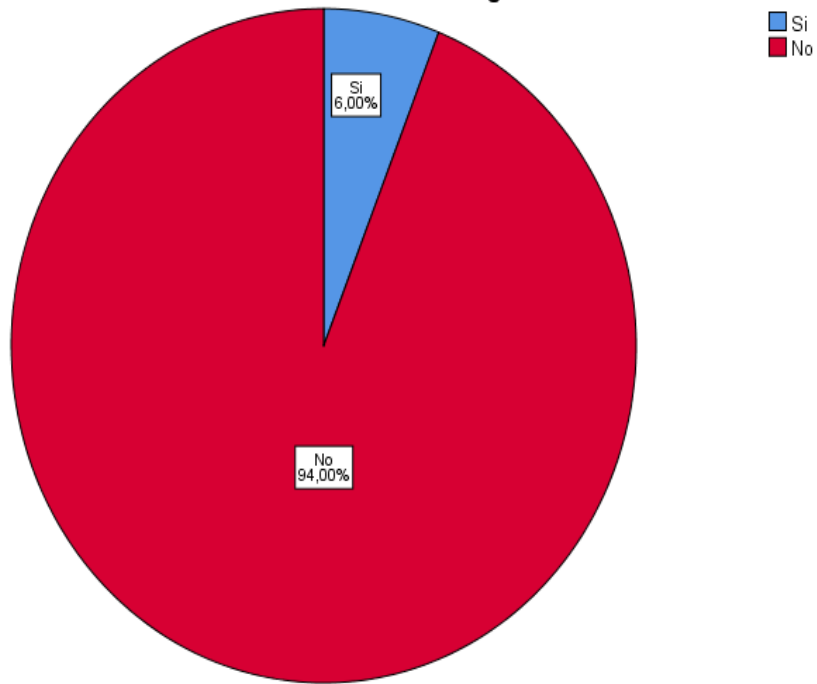
¿Considera usted que es importante monitorear las tarjetas de cuentas bancarias regularmente para la protección de los datos personales?



### Figura 11

Resultados de interpretación del ítem N° 10

¿Considera usted que las tarjetas virtuales son importantes para evitar las conductas fraudulentas del carding?



**Anexo 4. CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 1: "CARDING"**

N°	DIMENSIONES/ ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
	<b>DIMENSIÓN 1 Reintegración del penado</b>									
1	¿Conoce usted la figura del fraude que tiene como denominación el término carding?	X		X		X		X		
2	¿Considera usted que el fraude cibernético perjudica los derechos personales?	X		X		X		X		
3	¿Considera usted que el sistema de compra online es seguro en la comunidad?	X		X		X		X		
4	¿Considera usted que el carding viola los derechos basados en los datos personales de los individuos?	X		X		X		X		
5	¿Considera usted que el fraude cibernético perjudica a las empresas que venden por el sistema online?	X		X		X		X		

Observaciones (precisar si hay suficiencia<sup>4</sup>): aplicable \_\_\_\_\_

Opinión de aplicabilidad:  Aplicable  Aplicable después de corregir  No aplicable

Apellidos y nombres del juez validador: Mg Tovar Cerquen, Martin Vicente DNI: .....09700062.....

Especialidad del validador: ..... Gestión Publica .....

Lima sur, 10 de diciembre de 2024

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.

<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o Dimensión específica del constructo.

<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.

<sup>4</sup>Suficiencia: Los ítems son suficientes para medir la dimensión.



Firma del Experto Informante.

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 2: "DATOS PERSONALES"**

N°	DIMENSIONES/ ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
	<b>DIMENSIÓN 2 Gestión administrativa</b>									
1	¿Considera que la existencia de un mercado negro de compra de tarjetas robadas es la causa del carding?	X		X		X		X		
2	¿Considera usted que la consecuencia del fraude a nivel de suplantar datos en las tarjetas de crédito perjudica al titular de ella?	X		X		X		X		
3	¿Considera usted que el carding tiene consecuencias en las empresas financieras?	X		X		X		X		
4	¿Considera usted que es importante monitorear las tarjetas de cuentas bancarias regularmente para la protección de los datos personales?	X		X		X		X		
5	¿Considera usted que las tarjetas virtuales son importantes para evitar las conductas fraudulentas del carding?	X		X		X		X		

Observaciones (precisar si hay suficiencia<sup>4</sup>): si hay suficiencia \_\_\_\_\_

Opinión de aplicabilidad: Aplicable []      Aplicable después de corregir [ ]

Apellidos y nombres del juez validador: Mg Tovar Cerquen, Martin Vicente

No aplicable [ ]  
DNI: .....09700062.....

Especialidad del validador: .....Gestión Publica.....

Lima sur, 10 de diciembre de 2024

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.

<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o Dimensión específica del constructo.

<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.

<sup>4</sup>Suficiencia: Los ítems son suficientes para medir la dimensión.



Firma del Experto Informante.

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 1: "CARDING"**

N°	DIMENSIONES/ ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
	<b>DIMENSIÓN 1 Reintegración del penado</b>									
1	¿Conoce usted la figura del fraude que tiene como denominación el término carding?	X		X		X		X		
2	¿Considera usted que el fraude cibernético perjudica los derechos personales?	X		X		X		X		
3	¿Considera usted que el sistema de compra online es seguro en la comunidad?	X		X		X		X		
4	¿Considera usted que el carding viola los derechos basados en los datos personales de los individuos?	X		X		X		X		
5	¿Considera usted que el fraude cibernético perjudica a las empresas que venden por el sistema online?	X		X		X		X		

Observaciones (precisar si hay suficiencia<sup>4</sup>): hay suficiencia

Opinión de aplicabilidad: **Aplicable [x]**      **Aplicable después de corregir [ ]**

**No aplicable [ ]**

Apellidos y nombres del juez validador: Dra. CABRERA CUETO, YDA ROSA .....

DNI: .....06076309.....

Especialidad del validador: .....DRA EN DERECHO.....

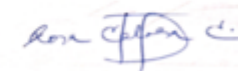
Lima sur, 15 de diciembre de 2024

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.

<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o Dimensión específica del constructo.

<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.

<sup>4</sup>Suficiencia: Los ítems son suficientes para medir la dimensión.



Firma del Experto Informante.

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 2: "DATOS PERSONALES"**

N°	DIMENSIONES/ ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
	<b>DIMENSIÓN 2 Gestión administrativa</b>									
1	¿Considera que la existencia de un mercado negro de compra de tarjetas robadas es la causa del carding?	X		X		X		X		
2	¿Considera usted que la consecuencia del fraude a nivel de suplantar datos en las tarjetas de crédito perjudica al titular de ella?	X		X		X		X		
3	¿Considera usted que el carding tiene consecuencias en las empresas financieras?	X		X		X		X		
4	¿Considera usted que es importante monitorear las tarjetas de cuentas bancarias regularmente para la protección de los datos personales?	X		X		X		X		
5	¿Considera usted que las tarjetas virtuales son importantes para evitar las conductas fraudulentas del carding?	X		X		X		X		

Observaciones (precisar si hay suficiencia<sup>4</sup>): si hay suficiencia

Opinión de aplicabilidad: Aplicable       Aplicable después de corregir

No aplicable

Apellidos y nombres del juez validador: Dra. CABRERA CUETO, YDA ROSA .....

DNI: .....06076309.....

Especialidad del validador: .....DRA EN DERECHO.....

Lima sur, 15 de diciembre de 2024

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.

<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o Dimensión específica del constructo.

<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.

<sup>4</sup>Suficiencia: Los ítems son suficientes para medir la dimensión.



\_\_\_\_\_  
Firma del Experto Informante.

**CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE 2: "DATOS PERSONALES"**

N°	DIMENSIONES/ ítems	Pertinencia <sup>1</sup>		Relevancia <sup>2</sup>		Claridad <sup>3</sup>		Suficiencia <sup>4</sup>		Sugerencias
		Si	No	Si	No	Si	No	Si	No	
	<b>DIMENSIÓN 2 Gestión administrativa</b>									
1	¿Considera que la existencia de un mercado negro de compra de tarjetas robadas es la causa del carding?	X		X		X		X		
2	¿Considera usted que la consecuencia del fraude a nivel de suplantar datos en las tarjetas de crédito perjudica al titular de ella?	X		X		X		X		
3	¿Considera usted que el carding tiene consecuencias en las empresas financieras?	X		X		X		X		
4	¿Considera usted que es importante monitorear las tarjetas de cuentas bancarias regularmente para la protección de los datos personales?	X		X		X		X		
5	¿Considera usted que las tarjetas virtuales son importantes para evitar las conductas fraudulentas del carding?	X		X		X		X		

Observaciones (precisar si hay suficiencia<sup>4</sup>):   hay suficiencia  

Opinión de aplicabilidad:   Aplicable [x]        Aplicable después de corregir []  

  No aplicable []  

Apellidos y nombres del juez validador:   Mg. Wilfredo Herbert Gordillo Briceño  

DNI:   08337343  

Especialidad del validador:   Gestión Pública  

Lima sur, 12 de diciembre de 2024

<sup>1</sup>Pertinencia: El ítem corresponde al concepto teórico formulado.

<sup>2</sup>Relevancia: El ítem es apropiado para representar al componente o Dimensión específica del constructo.

<sup>3</sup>Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es Conciso, exacto, y directo.

<sup>4</sup>Suficiencia: Los ítems son suficientes para medir la dimensión.



\_\_\_\_\_  
Firma del Experto Informante



**ANEXO 5. Cuestionario para encuesta.**

**CUESTIONARIO SOBRE EL CARDING Y LA PROTECCIÓN DE DATOS PERSONALES**

1. ¿Conoce usted la figura del fraude que tiene como denominación el término carding?
2. ¿Considera usted que el fraude cibernético perjudica los derechos personales?
3. ¿Considera usted que el sistema de compra online es seguro en la comunidad?
4. ¿Considera usted que el carding viola los derechos basados en los datos personales de los individuos?
5. ¿Considera usted que el fraude cibernético perjudica a las empresas que venden por el sistema online?
6. ¿Considera que la existencia de un mercado negro de compra de tarjetas robadas es la causa del carding?
7. ¿Considera usted que la consecuencia del fraude a nivel de suplantar datos en las tarjetas de crédito perjudica al titular de ella?
8. ¿Considera usted que el carding tiene consecuencias en las empresas financieras?
9. ¿Considera usted que es importante monitorear las tarjetas de cuentas bancarias regularmente para la protección de los datos personales?
10. ¿Considera usted que las tarjetas virtuales son importantes para evitar las conductas fraudulentas del carding?