UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO- UCAYALI, 2022

Tesis para optar el título profesional de

ABOGADO

TERESA LUCRECIA CATAÑO BARDALES

LINDA LUCERO PANDURO ARÉVALO

Pucallpa, Perú

2023

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
COMITÉ DE PLANEAMIENTO

ACTA DE EXAMEN DE GRADO PARA OPTAR EL TITULO DE ABOGADO

En la ciudad de Pucallpa, Siendo las 7:00 am del día Miércoles 08 de febrero del año 2023, en el auditorio de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de Ucayali, cito en el Pabellón I Segundo Piso, se dio inicio al EXAMEN DE GRADO, correspondiente a la sustentación de la tesis **"EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA DE CORONEL PORTILLO-UCAYALI 2022"** presentado por las Bachilleres en Derecho y Ciencias Políticas: **LINDA LUCERO PANDURO AREVALO Y TERESA LUCRECIA CATAÑO BARDALES.**

En cumplimiento del Reglamento de Grados y Títulos, el Secretario Académico de la Facultad procedió a presentar a los Miembros del Jurado integrados por los docentes: **Dr. EDGAR GUIZADO MOSCOSO** (Presidente), **DR. JOEL ORLANDO SANTILLAN TUESTA** (Miembro) y **Dr. ELADIO GUZMAN VILLA** (Miembro), designado con Memorando Múltiple N° 050/ 2023-UNU/FDyCP/GyT de fecha 24 de enero del 2023; luego del cual el señor presidente instó al Secretario Académico a presentar a las bachilleres examinadas.

Acto seguido el Presidente del Jurado invitó a las bachilleres a iniciar su exposición, de su informe final de tesis; a cuyo término los miembros del jurado las formularon las preguntas y objeciones respectivas, la misma que fue absuelta de forma SATISFACTORIA por las ponentes.

Continuando con el desarrollo de la sustentación y de conformidad con el Reglamento de Grados y Títulos, el presidente invitó a las bachilleres examinadas y al público asistente a abandonar la Sala para su correspondiente deliberación en forma reservada.

Seguidamente el Jurado emitió la calificación general, de cuyo resultado se establece que las bachilleres **LINDA LUCERO PANDURO AREVALO Y TERESA LUCRECIA CATAÑO BARDALES,** fueron **APROBADAS POR MAYORIA.**

Reiniciando el acto Público se realiza la Juramentación de honor y las felicitaciones de los miembros del Jurado, seguidamente se procedió a la lectura del presente acta, dando por concluido el acto de sustentación siendo a las 8:00am del mismo día, la suscribieron en señal de conformidad; de lo que doy fe.

Dr. EDGAR GUIZADO MOSCOSO
Presidente

Dr. JOEL ORLANDO SANTILLAN TUESTA
Miembro

Dr. ELADIO GUZMAN VILLA
Miembro

Dr. EUDOSIO PAUCAR ROJAS.
Secretario Académico

ACTA DE APROBACIÓN

La presente tesis fue aprobada por los miembros del Jurado Evaluador de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de Ucayali como requisito para optar el Título Profesional de Abogado.

Dr. Edgar Guizado Moscoso

Presidente

Dr. Joel Orlando Santillán Tuesta

Miembro

Dr. Eladio Guzmán Villa

Miembro

Dr. Teófilo Meza Taipe

Asesor

Bach. Teresa Lucrecia Cataño Bardales

Tesista

Bach. Linda Lucero Panduro Arévalo

Tesista

UNIVERSIDAD NACIONAL DE UCAYALI
VICERRECTORADO DE INVESTIGACION
DIRECCION DE PRODUCCION INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACION

SISTEMA ANTIPLAGIO URKUND

N° V/0801-2022

La **Dirección de Producción Intelectual**, hace constar por la presente, que el Informe Final de Tesis, **titulado:**

"EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO- UCAYALI, 2022".

Autor(es)	:	**CATAÑO BARDALES, TERESA LUCRECIA** **PANDURO ARÉVALO, LINDA LUCERO**
Facultad	:	DERECHO Y CIENCIAS POLÍTICAS
Escuela Profesional	:	DERECHO
Asesor (a)	:	Dr. TEÓFILO, MEZA TAIPE

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 10%.**

En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.

En señal de conformidad y verificación se firma y se sella la presente constancia.

FECHA 20/12/2022

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

UByP - REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, TERESA LUCRECIA CATAÑO BARDALES.

Autor(a) de la TESIS de pregrado titulada:

"EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO – UCAYALI, 2022"

Sustentada el año: 2023

Con la asesoría de: Dr. TEÓFILO MEZA TAIPE

En la Facultad de: DERECHO Y CIENCIAS POLÍTICAS.

Escuela Profesional de: DERECHO.

Autorizo la publicación:

PARCIAL [ ] Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL [X] Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempoy las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 09 / 02 / 2023

Email: teresalucresia@hotmail.com

Teléfono: 941873465

Firma:

DNI: 45626977

UNIVERSIDAD NACIONAL DE UCAYALI

UByP - REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, LINDA LUCERO PANDURO AREVALO.

Autor(a) de la TESIS de pregrado titulada:

"EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO - UCAYALI, 2022"

Sustentada el año: 2023

Con la asesoría de: Dr. TEÓFILO MEZA TAIPE.

En la Facultad de: DERECHO Y CIENCIAS POLÍTICAS.

Escuela Profesional de: DERECHO.

Autorizo la publicación:

PARCIAL [ ] Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL [X] Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempoy las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 09 / 02 / 2023

Email: pandurolindalucero@gmail.com

Teléfono: 920387612

Firma: Linda

DNI: 46948164

DEDICATORIA

Dedicamos el presente trabajo a nuestros familiares, quienes fueron motivo y apoyo durante todo este proceso de aprendizaje.

Las tesistas.

AGRADECIMIENTO

Agradecemos a Dios, por guiarnos y ser nuestra fortaleza en todo momento, y por brindarnos la oportunidad de lograr una de nuestras metas.

A nuestros padres, por su apoyo y amor incondicional y apoyarnos en nuestro proceso de formación profesional y personal, por los valores inculcados.

A los docentes de la Universidad Nacional de Ucayali por las enseñanzas y la motivación brindada.

A nuestro asesor, Dr. Teófilo Meza Taipe, por su tiempo invertido y su paciencia a pesar de sus recargadas labores, darnos una atención preferencial.

ÍNDICE DE CONTENIDO

Pág.

DEDICATORIA……vii

AGRADECIMIENTO……viii

ÍNDICE DE CONTENIDO……ix

ÍNDICE DE TABLAS……xiii

ÍNDICE DE FIGURAS……xiv

RESUMEN……xvi

ABSTRACT……xvii

INTRODUCCIÓN……xviii

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN 1

1.1. Planteamiento del Problema 1

1.2. Formulación del Problema 3

1.2.1. Problema General 3

1.2.2. Problemas Específicos 3

1.3. Objetivos…….. 4

1.2.1. Objetivo General 4

1.2.2. Objetivos Específicos 4

1.4. Justificación……. 5

1.4.1. Justificación Teórica 5

1.4.2. Justificación Práctica 5

1.4.3. Justificación Metodológica 6

1.5. Importancia …….. 6

1.6. Viabilidad……..... 6

1.7. Delimitación……. 7

1.7.1. Delimitación Temporal……7

1.7.2. Delimitación Teórica……7

CAPÍTULO II. MARCO TEÓRICO.....8

2.1. Antecedentes del Problema 8

2.2. Bases Teóricas……11

2.2.1. Delito Informático 11

2.2.1.1. Concepto y Tipicidad 11

2.2.1.2. Modalidad del Delito Informático 14

2.2.1.3. Características de los Delitos Informáticos.....18

2.2.2. Operaciones Financieras.....18

2.2.2.1. Concepto.....18

2.2.2.2. Riesgos Operacionales 19

2.2.2.3. Banca por Internet.....20

2.2.2.4. Operaciones Phishing 20

2.2.2.5. Gestión de riesgo 22

2.2.2.6. Otorgamiento de Crédito 22

2.3. Definicion de Términos Básicos 22

2.4. Formulación de Hipótesis… 24

2.4.1. Hipótesis General 24

2.4.2. Hipótesis Específicas.....25

2.5. Variables ……. 25

2.5.1. Variable X: Delito Informático 25

2.5.2. Variable Y: Operaciones Financieras 25

2.5.3. Operacionalización de las Variables 25

CAPÍTULO III. METODOLOGÍA 27

3.1. Método General 27

3.2. Tipo y Nivel de Investigación 27

3.3. Diseño de Investigación 28

3.4. Población y Muestra 29

3.5. Técnicas e Instrumentos de Recolección de Datos 31

3.6. Validación y Confiabilidad del Instrumento 31

3.7. Procedimiento de Recolección de Datos 31

3.8. Presentación de Datos 32

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 33

4.1. Descripcion de Resultados 33

4.2. Prueba de Hipótesis 47

4.3. Discusion de Resultados 55

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 57

5.1. Conclusiones 57

5.2. Recomendaciones 59

REFERENCIAS BIBLIOGRÁFICAS 60

ANEXO 64

Anexo 1. Matriz de Consistencia 65

Anexo 2. Matriz de instrumentos 66

Anexo 3. Instrumentos de Recolección de Datos 67

Anexo 4. Evidencias Fotográficas 69

ÍNDICE DE TABLAS

Pág.

Tabla 1. Operacionalización de variables…….. 26

Tabla 2. Categoría de análisis del coeficiente de correlación Rho de Spearman……. 32

Tabla 3. Prueba de correlación de Rho de Spearman de las variables delito informático y operaciones financieras……. 48

Tabla 4. Prueba de correlación de Rho de Spearman entre las variables delito informático y operaciones phishing……..……. 50

Tabla 5. Prueba de correlación de Rho de Spearman entre las variables Factores educativos y gestión de riesgo…… 52

Tabla 6. Prueba de correlación de Rho de Spearman entre las variables Factores social y otorgamiento de crédito……. 54

ÍNDICE DE FIGURAS

Pág.

Figura 1. ¿Cree usted que las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes?..... 33

Figura 2. ¿Considera que se debería desarrollar políticas de protección de información en las instituciones bancarias?..... 34

Figura 3. ¿En algún momento sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores?..... 35

Figura 4. ¿Usted fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas?..... 36

Figura 5. ¿Usted consideró que hicieron mal uso de su información personal las instituciones bancarias?..... 37

Figura 6. ¿Se siente vulnerable ante los estafadores por estar bancarizada?..... 38

Figura 7. ¿Llegó a ser víctima en algún momento de robo por medios electrónicos?..... 39

Figura 8. ¿Considera que el uso de aplicativos bancarios lo hace más propenso hacia las estafas?..... 40

Figura 9. ¿Considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea?..... 41

Figura 10. ¿Las instituciones bancarias deben desarrollar estrategias que cuiden a sus clientes ante posibles estafas o robos?..... 42

Figura 11. ¿Considera que se debería monitorear las operaciones sospechosas por las instituciones bancarias?..... 43

Figura 12. ¿Cree instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional?..... 44

Figura 13. ¿Consideras que las tarjetas de crédito deben contar con un seguro sin costos adicionales?..... 45

Figura 14. ¿Cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas?..... 46

RESUMEN

La Investigación titulada “El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia Coronel Portillo - Ucayali 2022”, y se planteó como objetivo de estudio, determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022, es una Investigación cuantitativa, de diseño no experimental, de nivel correlacional, en la que se planteó el siguiente problema general de estudio ¿ De qué manera el delito Informático incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo – Ucayali 2022?, teniendo como hipótesis general de estudio; el delito de información incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022 y sus variables de estudio son delito informático y operaciones financieras en la que se tiene como dimensiones de estudios acceso a una base de datos, uso ilegal de la información, operación Phishing, gestión de riesgo, otorgamiento de crédito; en la que se tiene como muestra de estudio a 263 personas bancarizadas de 18 a 70 años, a los que se aplicaron los cuestionarios y se conoció sus opiniones respecto al tema investigado y para la prueba de hipótesis se siguieron cinco pasos en la que se utilizó herramientas estadísticas descriptivas con un nivel de confiabilidad del 95%, con un Rho de Spearman 0.756 lo que indica la correlación positiva fuerte entre las variables de estudio.

Palabras claves: Delito informático, operaciones, financieras, phishing, gestión, riesgo, crédito, ilegal.

ABSTRACT

The investigation entitled "Computer crime and its impact on financial operations in the banks of the Coronel Portillo-Ucayali province 2022", and the objective of study was to determine how the crime of information affects financial operations in the banks of the province. province of Coronel Portillo - Ucayali 2022, is a quantitative investigation, of non-experimental design, of correlational level, in which the following general problem of study was raised: How does computer crime affect financial operations in banks of the province? colonel portillo province - Ucayali 2022?, having as a general study hypothesis the crime of information has a significant impact on financial operations in the banks of the Coronel Portillo province - Ucayali 2022 and its study variables are computer crime and financial operations in which has as dimensions of studies access to a database, illegal use of information, Phishing operation, risk management, credit granting. In which the study sample is 263 banked people from 18 to 70 years old, to whom the questionnaires were applied and their opinions regarding the investigated topic were known and for the hypothesis test, five steps were followed in which it was used descriptive statistical tools with a reliability level of 95%. with a spearman's rho 0.756, which indicates the strong positive correlation between the study variables.

Keywords: Computer crime, operations, financial, phishing, management, risk, credit, illegal.

INTRODUCCIÓN

El avance de la tecnología se da a pasos agigantados y a raíz de ello las relaciones comerciales y sociales han dado un giro de 360 grados con las nuevas tecnologías, por ello es lógico pensar que el nuevo contexto de desarrollo de las personas se dan en este entorno que muchas veces facilita el desarrollo de su vida cotidiana, sin embargo estos avances vienen acompañados de diversos delitos que tiene como herramienta principal la computadora y las diversas plataformas digitales, actualmente existe una amplia variedad de delincuencia informática, que se está expandiendo rápidamente dejando indefensos a miles de personas, el uso de medios informáticos les permite a los delincuentes cometer estos delitos sin ser identificados, ni sancionados ya que saben que las redes electrónicas son totalmente manipulables en la cual la información personal y económica de las personas se encuentran vulnerables y son aprovechados por los delincuentes cibernéticos que realizan sus fechorías sin ninguna impunidad y a raíz del Covid-19 muchas personas en el país y la Región fueron víctimas de este delito, por ende el presente trabajo busca conocer la relación entre el delito informático y las operaciones financieras.

El presente trabajo de investigación siguió la siguiente estructura:

El capítulo I. despliega el planteamiento del problema a investigar, los objetivos, la justificación, la importancia y las delimitaciones de la investigación.

El capítulo II. Está compuesta por los antecedentes internacionales, nacionales y locales; además por el marco teórico de cada variable de estudio, las definiciones de términos básicos y las hipótesis, variables y la operacionalización de las variables,

El capítulo III. Abarca la metodología de investigación, el diseño, nivel, tipo y enfoque de investigación, así como la población, muestras, lugar de ejecución y tratamiento de datos.

El capítulo IV, alcanza los resultados, la prueba de hipótesis y discusión de resultados.

En el capítulo V, se muestran las conclusiones y recomendaciones

Por último se presentan las referencias bibliográficas y los anexos de la investigación.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del Problema

En la actualidad, el uso de la tecnología se ha masificado en la sociedad, diseñando nuevos hábitos en nuestra manera de vivir y nos permite realizar muchas actividades desde nuestros hogares; pero así como a implicado ciertas facilidades en nuestras tareas, también ha expuesto la información personal del individuo, ya que actualmente no hay una persona que no tenga en su poder un teléfono celular y por lo cual, acceso a internet, siendo vulnerables para aquellas personas inescrupulosas tengan acceso al manejo de nuestra información, generando un sin fin de riesgos dentro de las cuales resaltan el robo de información personal mediante los correos electrónicos, accesos a internet, redes sociales, etc., lo que vulnera la seguridad y la privacidad de información de las personas.

La información personal se vio expuesta en un mayor nivel durante la cuarenta por COVID-19, que afectó al mundo entero, y al estar encerrados por tanto tiempo y no poder realizar ciertas actividades ya sea del pago de sus servicios básicos, así como las compras diarias de alimentos, lo que en gran medida puso en riesgo que delincuentes cibernéticos detectaran con mayor facilidad a sus víctimas y resultado de ello son los delitos cibernéticos que han crecido de manera exuberante, siendo las personas que tiene su dinero en los bancos o una tarjeta de crédito las que se vieron afectadas por la delincuencia cibernética, ya que muchas veces las entidades financieras no se hacen cargo

de las pérdidas que sus clientes puedan tener, ya sea por el robo de sus ahorros o compras realizadas con sus tarjetas de crédito, al final del caso las entidades bancarias no reconocen y sus clientes pierden su dinero.

El delito informático está en aumento, porque “La Policía Nacional del Perú (PNP) registró 14 mil 671 denuncias por delitos informáticos durante el año 2021. Esto representa un aumento de 65% de casos más que el año anterior 8 897 denuncias en 2020” (Perú, 2022).

Esta situación va en aumento, ya que las instituciones financieras no dan la garantía y /o protección a sus clientes ya que a diario escuchamos o vemos en los medios de comunicación que una banda cibernética con modalidades y equipos modernos irrumpen en sus sistemas vulnerando la información de sus clientes de los cuales esto no se hacen cargo al momento de reembolsar las pérdidas económicas de sus clientes.

Andina (2022), informa sobre el incremento de los delitos informáticos:

Delito informático	2020	2021	2022
Delitos contra datos y sistemas informáticos	437	591	138
Delitos informáticos contra la indemnidad y libertad sexual	76	120	29
Delitos informáticos contra la intimidad y el secreto de las comunicaciones	345	479	101
Fraude informático	**5420**	**11810**	**3827**
Suplantación de identidad	**751**	**3429**	**946**
Disposiciones comunes y agravantes	75	389	162
Otros	2538	1827	153
Estafa agravada para acceder o sustraer datos del tarjetas de ahorro o crédito	178	456	110

Y nuestra Región de Ucayali no escapa a esta cruda realidad, cuando se presenta la denuncia ante las instituciones financieras estas se deslindan de toda responsabilidad aludiendo que el cliente no cuenta con un seguro que cubra dichas pérdidas o ingresan un reclamo que demora en ser atendidos más de un mes en las que al final simplemente dan como infundados dicho reclamo, y cuando se hace llegar esta denuncia a las instituciones correspondiente (Comisaría, Poder Judicial) no siempre se logra que la persona afectada recupere su dinero perdido.

Es por ello que mediante la presente investigación buscamos conocer como el delito informático incide en las operaciones financieras de los bancos de la provincia de Coronel Portillo - Ucayali 2022, y, qué medidas se deberían tomar para responsabilizar de alguna manera a las instituciones bancarias para hacer frente a esta vulnerabilidad de datos de las personas.

1.2. Formulación del Problema

1.2.1. Problema General

- ¿De qué manera el delito informático incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo – Ucayali 2022?

1.2.2. Problemas Específicos

- ¿En qué medida el delito informático incide en las operaciones phishing de los bancos de la provincia de Coronel Portillo - Ucayali 2022?

- ¿En qué medida el delito informático se relaciona con la gestión de riesgos en los bancos de la provincia de Coronel Portillo – Ucayali 2022?
- ¿En qué medida el delito informático incide en la vulnerabilidad de los créditos otorgados por los bancos de la provincia de Coronel Portillo - Ucayali 2022?

1.3. Objetivos

1.3.1. Objetivo General

- Determinar como el delito informático incide en las operaciones financieras de los bancos en la provincia de Coronel Portillo - Ucayali 2022.

1.3.2. Objetivos Específicos

- Determinar en qué medida el delito informático incide en las operaciones Phishing de los bancos de la provincia de Coronel Portillo - Ucayali 2022.
- Determinar en qué medida el delito informático tiene relación con la gestión de riesgos de los bancos de la provincia de Coronel Portillo - Ucayali 2022.
- Determinar en qué medida el delito informático incide en la vulnerabilidad de los créditos otorgados por los bancos de la provincia de Coronel Portillo - Ucayali 2022.

1.4. Justificación

1.4.1. Justificación Teórica

El delito informático es una acción que se da por vías informáticas vulnerando la información privada de las personas y hacer uso indebido de los mismos para cometer un robo, estafa, etc., que pueda dañar y ocasionar pérdidas económicas a las personas, a través de las instituciones financieras que si bien es cierto también son las que salen perjudicadas, estas no garantizan la seguridad de sus clientes en cuanto al robo, desligándose de toda responsabilidad y no responden a aquellas operaciones realizadas vía internet, por lo cual la investigación tratará de conocer como el delito informático incide en las operaciones financieras de los bancos en Ucayali.

1.4.2. Justificación Práctica

La presente investigación es relevante por cuanto en nuestra actualidad de avances tecnológicas y previa a la cuarentena por COVID-19, la gran mayoría de personas en especial las que tienen cuentas en el sistema financiero realizan sus operaciones desde casa, siendo más vulnerables a robos de información sin que las entidades bancarias se den cuenta de las transacciones inusuales y puedan proteger y salvaguardar los ahorros de sus clientes, así mismo se espera que el presente estudio sirva de modelo para futuras investigaciones en el campo.

1.4.3. Justificación Metodológica

La presenta investigación buscó conocer la problemática en cuanto a las variables de investigación mediante proceso que conllevaran a la recopilación y análisis de información, en cuanto al delito informático y su incidencia en las operaciones financieras de los bancos de la Provincia de Coronel Portillo - Ucayali 2022, para lo cual, se usaron las herramientas necesarias de indagación, con el fin plantear estrategias de solución a la problemática en estudio.

La investigación utilizó los conocimientos científicos con el propósito de crear nuevos conocimientos sobre el delito informático en el ámbito penal.

1.5. Importancia

La investigación buscó identificar cuáles son las causas por las que el delito informático afecta a las operaciones financieras de los bancos con las que se vulneran la información personal de los clientes y estén en peligro de ser víctimas de robos, estafas y suplantación de sus identidades sin que los entes correspondientes brinden la seguridad y garantía de que su dinero e información personal estén protegidos ante este peligro.

Los bancos deberían brindar las garantías y soporte ante estos delitos a sus clientes y respaldar las pérdidas económicas que puedan sufrir.

1.6. Viabilidad

Esta investigación fue viable porque contamos con todos los recursos necesarios para efectuar el estudio, tales como materiales, economías,

disponibilidad de tiempo y entusiasmo para llevarla a cabo.

1.7. Delimitación

1.7.1. Delimitación Temporal

En la presente investigación se usó información que corresponda al periodo 2022.

1.7.2. Delimitación Teórica

La investigación que se realiza abarco únicamente los temas el delito informático y las operaciones financieras de los bancos.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes del Problema

2.1.1. Antecedentes Internacionales

Chiluisa (2021) en su estudio titulado “Los delitos informáticos y los vacíos legales que afectan a los ciudadanos” Universidad Católica de Santiago de Guayaquil” - Ecuador. en la cual se tuvo como objetivo Elaborar un ensayo crítico jurídico en evidencia de los vacíos legales existentes en el ordenamiento jurídico ecuatoriano y que tienen relación con los delitos informáticos que actualmente afectan a los ciudadanos y se obtuvo los siguientes resultados debido a que la mayor parte de la población maneja y usa tecnología y es justamente por medio de las redes informáticas que se vuelve vulnerable la información que cada una de las personas confiere o comparte en las plataformas electrónica, por lo cual la delincuencia común ha transcendido en un nuevo tipo de delincuencia organizada que usa la tecnología para beneficio y lucro propio, la mayor parte de estos delitos quedan en la impunidad al no haber un procedimiento adecuado para proveer su comisión.

Morán y Morán (2020), en su estudio titulado “Delitos informáticos, reforma al artículo 190 ce COIP en el contexto de la emergencia sanitaria Ecuador 2020”, Universidad de Guayaquil – Ecuador, en la se tuvo como objetivo de investigación realizar una investigación profunda sobre el fenómeno de las infracciones informáticas y se tuvo los siguientes resultados: Los delitos informáticos tienen una evolución constante y que debido a los nuevos contextos en los que se interactúan es necesario tipificar los actos delictivos que con la

ayuda tecnológica se cometen, actualmente el código orgánico integral penal de ecuador ha tenido un gran avance al establecer delitos informáticos, pero que es necesario una revisión periódica para actualizarlo al ritmo que aparecen nuevos delitos informáticos, no existen cifras que permitan visualizar la real situación de los delitos informáticos en el país y estos pueden afectar desde cualquier lugar remoto del planeta.

2.1.2. Antecedentes Nacionales

Mori (2019) en su estudio titulado “Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, Periodo 2008 al 2012” de la Universidad Nacional Federico Villarreal, Perú, en la que se llegó a las siguientes conclusiones; para conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad, se encontró que los jueces aceptan que existe ausencia de formación tecnológica en delitos informático, pero los fiscales y policías dicen estar en desacuerdo, también los jueces aceptan que existe desconocimiento de la tecnología, para los fiscales son indiferentes, los jueces y fiscales aceptan que hay transgresiones de las legislaciones vigentes, los jueces están de acuerdo con la impropia determinación del tipo penal, los fiscales en desacuerdo al igual que los policías, para determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad, se encontró que la deontología tecnológica que afecta a competitividad de los operadores de justicia influye en la impropia determinación

del tipo penal y en la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

De La Cruz (2021), en su estudio titulado “Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la Provincia de Huaura - Huacho 2018”, de la Universidad José Faustino Sánchez Carrión - Perú, al que se llegó a las siguientes conclusiones, en la que el 86% considera que el sistema financiero y bancario frente a los fraudes debe ser el sistema bancario y financiero quien debe responder a favor de sus clientes, aun cuando el cliente no contrate un seguro, el 94% considera que las operaciones financieras por internet se relaciona de manera significativa con la responsabilidad civil de los bancos, las posiciones teóricas y estadísticas asumen que un 79% considera que, no se justifica que los bancos no asuman la gestión de los riesgos en la atención a los clientes mediante la banca por internet.

2.1.3. Antecedentes Locales

Marín y Santa María (2019), en su estudio titulada “El ciber delito de redes delictivas a escala global a entidades gubernamentales y la responsabilidad del órgano de control interno en una Municipalidad de la Región de Ucayali, año 2020”, de la Universidad Nacional de Ucayali - Perú y se llegó a las siguientes conclusiones, que hay una estrecha relación entre los riesgos tecnológicos y la implementación de un área de prevención con un auditorio interno antifraude de los fondos de las municipalidades distritales o Provinciales, de los resultados obtenidos el 92% está completamente de acuerdo que los riesgos tecnológicos tienen relación la implementación de un área de prevención con un auditorio

interno antifraude de los fondos, el 1.10% no sabe al respecto, también hay una estrecha relación entre riesgo de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las Municipalidades Distritales o Provinciales, además los resultados obtenidos el 68.20% está completamente de acuerdo los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos, el 1.10% no sabe al respecto, también hay una estrecha relación entre el riesgo informático en el desvió de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales. Así mismo los resultados muestran que el 89.70% está completamente de acuerdo que los riesgos informáticos en el desvió de fondos y la obtención de una seguridad razonable del control interno el 1.10% no sabe al respecto.

En cuanto a la variable operaciones informáticas no existe estudios previos en el ámbito local.

2.2. Bases Teóricas

2.2.1. Delito Informático

2.2.1.1. Concepto y Tipicidad

Los delitos informáticos, son delitos especiales legislados mediante Ley Nº 30096, que tiene por objeto:

… prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia (art. 1).

Vilca (2018) “Acción, típica, antijuridica y culpable que se da por vías informáticas o que tienen como objetivo distribuir“ (p. 21).

La inseguridad ciudadana se entiende a como la sensación de miedo y preocupación individual de sufrir desgracias o delitos, relacionados estos con dañar ordenes, medios electrónicos de internet (p. 21).

Mori (2019) “Acción ilegal en el que el ordenador es el instrumento o el objeto del delito y más concretamente, cualquier delito ligado al tratamiento automático concretamente de datos (p. 20).

Así mismo, afirma Mori (2019), “es el acto relacionado con la tecnología informática por el cual una víctima ha sufrido una perdida y un autor ha obtenido intencionalmente una ganancia (p. 20).

Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático, el delito informáticos implica actividades criminales que en un primer momento los países han tratado de cuidar en figuras de carácter tradicional, así como robo, hurto, fraude, falsificaciones, perjuicio, estafa, sabotaje, entre otros, sin embargo debe desatacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho (Blossiers, 2018, p. 52).

Es el acto consciente y voluntario que genera un perjuicio voluntario a personas naturales o jurídicos, no llevando necesariamente a un beneficio material a su autor, por el contrario, produce un beneficio ilícito para su autor aun siendo no perjudica a la víctima, en cuya comisión interviene indispensablemente de activa dispositivos normales utilizado en las actividades informáticas (Vilca, 2018, p. 42).

Los delitos informáticos están tipificados en variedad de modalidades como, ataques contra sistemas y datos informáticos, usurpación de identidad, distribución de imágenes de agresiones sexuales contra menores, estafas a través de internet, intrusión en servicios financieros en línea, difusión de virus botones, redes de equipos infestados controlados por usuarios remotos y el Phishing (adquisidor fraudulenta de información personales confidencia (Alarcón y Barrera, 2017, p. 71).

El delito informático es perpetuado por el uso de computadora a través de redes y sistemas de información sistematizada, independiente del propósito y finalidad deseada por parte del criminal o delincuente informático, es preciso, resulta que el delito informático existe dentro del marco jurídico la acción de los sujetos que intervienen en ellas por ello tipifican dos que son sujetos activos y sujetos pasivos, de acuerdo a ello se conceptúa de la siguiente forma (Alarcón y Barrera, 2017, p. 72).

Por su parte, Costa y Ruiz (2016), indica que “son aquellas conductas ilícitas susceptibles de ser sancionadas y el derecho penal que hacen uso indebido de cualquier medio informático” (p. 34).

El delito informático implica actividades criminales que los países han tratado en encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotaje, también debe destacarse que el uso de las técnicas de información ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regular por parte del derecho.

Por otro lado, Costa y Ruiz (2016) menciona “como la apropiación de información y la intimidad personal en las redes sociales y debe considerarlo

acto antijuridico y se causa de sanción y considerárselo como delito informático, dado que afecta la privacidad de una persona y el colectivo en general” (p. 9).

2.2.1.2. Modalidades del Delito Informático

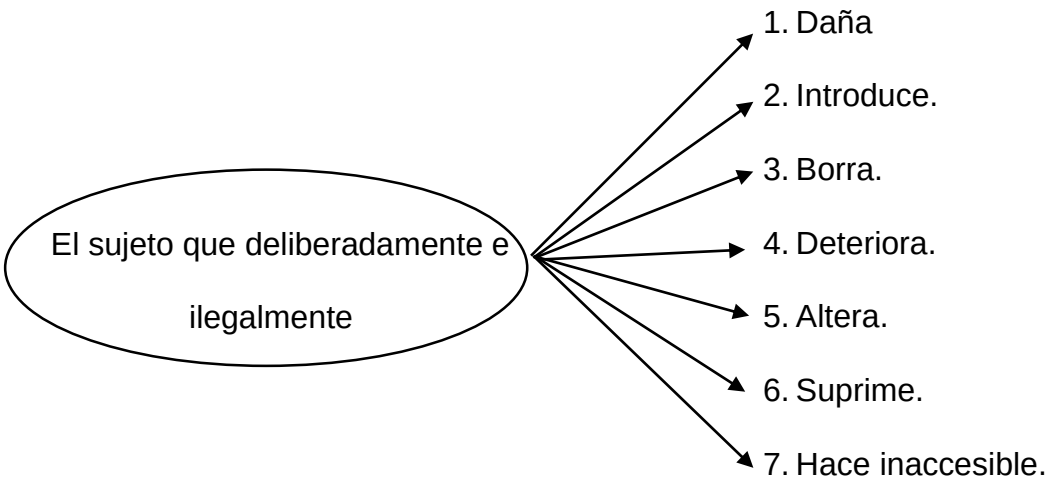
2.2.1.2.1. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo (…) el que accede a un sistema informático excediendo lo autorizado (art. 2, Ley Nº 30096).

2.2.1.2.2. Atentado a la integridad de los datos informáticos

“El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa” (art. 3, Ley Nº 30096).

El verbo rector:



2.2.1.2.3. Atentado contra integridad del sistema informático

El atentado contra la integridad del sistema informático, se produce cuando el sujeto activo “que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios…” (art. 4, Ley Nº 30096), la sanción que establece por este delito “… será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa”.

En general, se entiende como criminalidad informática aquella conducta dirigida a burlar los sistemas de dispositivos de seguridad esto es el ingreso no autorizado a computadoras, correos o sistemas de data mediante clave de acceso la destrucción o daño a bases de datos, programas, etc., estos delitos tiene las características que solo pueden ser cometidas por medios de sistemas informáticos (Hancco, 2017, p. 30).

Así mismo, Hannco (2017) argumenta que “el delito informático en un sentido amplio comprende todas aquellas conductas que las TIC son el medio de ejecución del delito, la comisión de estos actos delictuosos plantea la especialización de los individuos que las cometen (p. 30).

2.2.1.2.4. Fraudes informáticos

Los sujetos buscan alguna ventaja patrimonial, la norma regula como la conducta implica el diseño alteración, borrado, supresión, clonación o alteración del sistema informático a efectos de mantener en error a la víctima y en esa circunstancia aprovecharse ilícitamente, esta modalidad se da cuando se clonan

páginas web de entidades financieras con el fin de obtener los datos financieros de las víctimas y sustraer sumas de dinero y efectuar comprar en perjuicio de las victimas (Hancco, 2017, p. 30).

La Ley Nº 30096 es su artículo 8 establece el sujeto que en forma "deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático".

2.2.1.2.5. Interceptación de datos informáticos

El sujeto que en forma "deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos" (art. 7, Ley Nº 30096).

2.2.1.2.6. Manipulación de datos de entrada

Consiste en la sustracción de códigos y claves que las victimas utilizan para el ingreso a almacenamiento de datos, acceso a programas, entre otros, se caracteriza por la obtención de información esto de genera cuando la víctima accede a determinados programas, páginas web, donde previamente se ha condicionado el sistema para la sustracción y / o manipulación de la información, esto puede suceder cuando se clona la página web de una entidad financiera a efectos de obtener los datos de las tarjeras de créditos (Hancco, 2017, p. 32)

2.2.1.2.7. Manipulación de datos de salida

Hancco (2017), este delito incide en la información o datos que la víctima obtiene del sistema informático esta falsa información permite a los delincuentes aprovecharse del error y que se encuentra la victima a efectos de conseguir determinados beneficios (p. 32).

2.2.1.2.8. Manipulación de programas

Este tipo de delito los delincuentes buscan que los programas informáticos que tiene el ordenador de la víctima realicen actividades ordenadas por el agente del delito buscando determinada beneficio, para ello va a alterar el funcionamiento de programas informáticos con la finalidad de obtener algún tipo de beneficio (Hancco, 2017, p. 33).

Hancco (2017), “Una de las formas es el uso de troyanos que son programas que ingresan bajo un disfraz de un programa solicitado, sin embargo, en el sistema de la víctima empieza a ejecutar el programa oculto que por lo general busca el control remoto del ordenador de las víctimas” (p. 30).

2.2.1.2.9. Suplantación de identidad

La persona que “mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral…” será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años (art. 9 Ley Nº 30096).

2.2.1.3. Características de los Delitos Informáticos

De acuerdo a Blossiers (2018), las características de los delitos informáticos son las siguientes**:**

- Conductas criminales de cuello blanco.
- Acciones ocupacionales.
- Acciones de oportunidad.
- Provocan pérdidas económicas.
- Muchos casos y pocas denuncias.
- Proliferación continua.
- Ilícitos de impunidad ante la ley.
- Delitos que genera robos por medio de tarjeta de crédito.
- Sistemas impersonales.
- Fraudes que son deficientes de equiparar (Blossiers, 2018, p. 28).

2.2.2. Operaciones Financieras

2.2.2.1. Concepto

Son aquellas operaciones efectuadas por la entidades financieras para captar y colocar recursos de manera profesional esto es permanente y masiva por cuanto corresponde al objeto social propia de estas instituciones financieras, las operaciones financieras están divididas en dos grupos, la primera llamadas fundamentales o típicas que corresponde en el fondo a las realizaciones de un negocio de crédito y las otras denominadas complementarias o accesorias, agrupan todas las demás que prestan las entidades bancarias (Arteaga y Choquehuanca, 2017, p. 45).

“Una operación financiera es todo intercambio no simultáneo de capitales financieros pactado entre el prestamista y el prestatario siempre que se verifique la equivalencia, en base una ley financiera, entre los capitales entregados por uno y otro” (López, 2020).

Las operaciones financieras son instrumentos que permiten a personas físicas o jurídicas un intercambio de capitales en diferentes momentos del tiempo, quien tienes los siguientes elementos:

- **Personal:** Elemento personal es el sujeto activo el que dispone de liquidez que acede que otros utilicen durante un tiempo y el sujeto pasivo es el que recibe y utiliza.
- **Material:** está constituido por el capital financiero o de moneda en cantidad “C“ y el tiempo de uso “T”.
- **Convencional o formal:** La Ley de equilibrio de mercado.

2.2.2.2. Riesgos operacionales

Este peligro inicia cuando coexiste la eventualidad de error o perjuicio a causa de los procesos de aceptación, procesos de realización y acumulación de informes, como a las personas encargadas de su administración, las diferencias respecto al tema de protección son altamente significativas, dado que las entidades bancarias pueden padecer agresiones en cuanto a métodos o efectos, este mal uso de peligro operacional también se puede aparecer del lado del consumidor, o por algún método inadecuado de la banca en línea (De La Cruz, 2021, p. 27).

2.2.2.3. Banca por Internet

De acuerdo a la resolución administrativa circular 046-2010 del BCRP, es también conocida como M-Banking (Mobile Banking) o banca por celular, la cual radica en la ejecución de transacciones bancarias por medio de los teléfonos celulares, la banca por internet reconoce a los consumidores bancarios la conducción de sus cuentas aun en sitios retirados, siempre que tengan con la cubierta de la prestación de telefonía celular (De La Cruz, 2021, p. 40).

La tecnología actualmente hace que la banca móvil sea un dispositivo por medio de cual pueda utilizarse el dinero electrónico para la ejecución de diligencias de forma virtual y desechando la utilización del dinero en efectivo o de otras formas, como las transacciones cibernéticas con lo que se proporciona a los clientes el dominio de verificar las adquisiciones y desembolsos de cualquier modalidad desde cualquier sitio usando solo el teléfono móvil (De La Cruz, 2021, p. 41)

De La Cruz (2021), también indica que se “define a este acuerdo como el concedes recurrir a las prestaciones y productos utilizable de una institución bancaria vía online (p. 41).

2.2.2.4. Operaciones Phishing (D1)

Los phishing simulan pertenecer a entidades bancarias de reconocidos prestigios y solicitan a los ciber navegantes datos de tarjetas de crédito o claves bancarias mediante un formulario o un correo electrónico con un enlace que conduzca a una falsa página web, con una apariencia similar a la de la web original, en este caso es el propio incauto internauta quien proporciona los datos

requeridos permitiendo al autor del ilícito lograr un beneficio económico ilegitimo (Mori, 2019, p. 91)

“El phishing es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas” (Belcic, 2020).

También es conocida como robo de identidad, esta modalidad de fraude consiste en él envió de supuestas promociones y ofertas comerciales que la víctima debe aceptar insertando sus datos en los formularios simulados que enviaran la información a los delincuentes y estos con dicha información obtendrán beneficios con perjuicio de la víctima que cuando revise su estado de cuenta recién se dará cuenta del delito del cual ha sido objeto (Hancco, 2017, p. 33).

El phishing es un tipo de engaño creado por hackers, pero en este caso con fines delictivos para obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc., generalmente, el engaño se basa en la ignorancia del usuario porque ingresa a un sitio que presume real, autentico o que es el legal.

El ciberdelincuente ataca:

Su ataque se dirige:	- Comunicación electrónica. - Correo electrónico. - Llamada telefónica
Se hace pasar como:	- Persona natural o jurídica
Su objetivo es obtener:	- Información personal - Información confidencial. - Credenciales de inicio de sesión. - Obtener Nº de tarjeta de crédito

2.2.2.5. Gestión de Riesgo (D2)

Utiliza las tácticas que consiente efectuar el sistema de control interno en las instituciones públicas y privadas transgrediendo en la gestión de riesgos, formando definiciones, procedimientos y métodos expresados por los entes de control para corregir o mejorar los riesgos (De La Cruz, 2021, p. 49).

2.2.2.6. Otorgamiento de Crédito (D3)

Movimiento financiero mediante la cual un acreedor facilita determinada cantidad de dinero a otro, al cual se le denomina deudor, quien se compromete a devolver dicha cantidad en un tiempo determinado sumándole un monto más que es el interés del préstamo (De La Cruz, 2021, p. 49).

2.3. Definición de Términos Básicos

- **Banca por internet:** De La Cruz (2021) también indica que se “define a este acuerdo como el concedes recurrir a las prestaciones y productos utilizable de una institución bancaria vía online (p. 41).

- **Delito informático:** Vilca (2018) “Acción, típica, antijuridica y culpable que se da por vías informáticas o que tienen como objetivo distribuir” (p. 21).

- **Fraudes:** Implica el diseño alteración, borrado, supresión, clonación o alteración del sistema informático a efectos de mantener en error a la víctima y en esa circunstancia aprovecharse ilícitamente, esta modalidad

se da cuando se clonan páginas web de entidades financieras con el fin de obtener los datos financieros de las víctimas y sustraer sumas de dinero y efectuar compras en perjuicio de las víctimas (Hancco, 2017, p. 30).

- **Gestión de riesgo:** Utiliza las tácticas que consiente efectuar el sistema de control interno en las instituciones públicas y privadas transgrediendo en la gestión de riesgos, formando definiciones, procedimientos y métodos expresados por los entes de control para corregir o mejorar los riesgos (De La Cruz, 2021, p. 49).

- **Manipulación de datos de entrada:** Consiste en la sustracción de códigos y claves que las victimas utilizan para el ingreso de almacenamiento de datos, acceso a programas, entre otros (Hancco, 2017, p. 32).

- **Manipulación de datos de salida:** Hancco (2017), este delito incide en la información o datos que la víctima obtiene del sistema informático, esta falsa información permite a los delincuentes aprovecharse del error y que se encuentra la victima a efectos de conseguir determinados beneficios (p. 32).

- **Operación financiera:** Arteaga y Choquehuanca (2017), “Son aquellas operaciones efectuadas por la entidades financieras para captar y colocar recursos de manera profesional esto es permanente y masiva por cuanto corresponde al objeto social propia de estas instituciones financieras, las operaciones financieras” (p. 45).

- **Otorgamiento de créditos:** Movimiento financiero mediante la cual un acreedor facilita determinada cantidad de dinero a otro, al cual se le denomina deudor, quien se compromete a devolver dicha cantidad en un tiempo determinado sumándole un montón mas que es el interés del préstamo. (De La Cruz, 2021, p. 49).

- **Phishing:** El phishing es un tipo de engaño creado por hackers, pero en este caso con fines delictivos para obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc., generalmente, el engaño se basa en la ignorancia del usuario porque ingresa a un sitio que presume real, autentico o que es el legal (Duran y Duran, s.f.).

- **Smishing:** Una variante del *phishing* a través de los sistemas de mensajería instantánea y de los mensajes de texto (SMS) (Andina, 2022).

- **Vishing:** Usando la vía telefónica se busca engañar al usuario para que ofrezca su información personal sin que note la estafa (Andina, 2022).

2.4. Formulación de Hipótesis

2.4.1. Hipótesis General

- El delito informático incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022.

2.4.2. Hipótesis Específicas

- Existe incidencia entre el delito informático y las operaciones phishing en los bancos de la provincia de Coronel Portillo – Ucayali 2022.
- Existe relación entre el delito informático y la gestión de riesgos en los bancos de la provincia de Coronel Portillo – Ucayali 2022.
- Existe incidencia entre el delito informático y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022.

2.5. Variables

2.5.1. **Variable X:** Delito Informático.

Dimensiones:

- X1: Acceso a una base de datos.
- X2: Uso ilegal de la información.

2.5.2. **Variable Y:** Operaciones Financieras.

Dimensiones:

- Y1: Operación Phishing.
- Y2: Gestión de riesgo.
- Y3: Otorgamiento de crédito.

2.5.3. Operacionalización de las variables

Se describe en la siguiente tabla:

Tabla 1

Operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Delito Informático	Vilca (2018) “Acción, típica, antijuridica y culpable que se da por vías informáticas o que tienen como objetivo distribuir “ (p.21)	El delito informático se da cuando vulneran la información privada de las personas para realizar robos, fraudes económicos que se llevan a cabo mediante los medios tecnológicos.	**X1:** Acceso a una base de datos **X2:** Uso ilegal de la información	**X1.1** Vulnerabilidad de los datos **X1.2.** Vulnerabilidad de la información personal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca
Operaciones Financieras	Arteaga y Choquehuanca (2017), “Son aquellas operaciones efectuadas por las entidades financieras para captar y colocar recursos de manera profesional esto es permanente y masiva por cuanto corresponde al objeto social propia de estas instituciones financieras, las operaciones financieras” (p.45)	Las operaciones financieras son transacciones económicas que se realizan en instituciones financieras en la que el dinero juega el papel más importante. .	**Y1:** Operaciones Phishing **Y2:** Gestión de riesgos **Y3:** Otorgamiento de Créditos	**Y1.1.** Captación mediante internet **Y2.1**.Monitoreo de procesos **Y2.2.** Estrategias de control **Y3.1.** Desembolsos de préstamos **Y3.2.** Otorgamientos de tarjetas de crédito	- Siempre - Casi siempre - A veces - Casi nunca - Nunca

CAPÍTULO III

METODOLOGÍA

3.1. Método General

Como método general se utilizó el método inductivo y deductivo.

Método inductivo, para Ander - Egg (1995), “es un proceso que parte del estudio de casos particulares para llevarlos a conclusiones o leyes universales que explican un fenómeno” (p. 200).

Método deductivo, según Ander - Egg (1995) “es el razonamiento que, partiendo de casos particulares, se elevan a conocimientos generales” (p. 98).

3.2. Tipo y Nivel de la Investigación

3.2.1. Tipo de Investigación

La investigación fue de tipo mixto, aplicada porque se partirá de una hipótesis, se utilizó la observación, para contrastar las hipótesis y corroborar las teorías existentes, la investigación básica también es conocida como la investigación pura la cual lleva los conocimientos básicos a la realidad teórica (Paucar, 2020).

Según en el tiempo; fue transversal porque lo realizamos durante el año 2022. De acuerdo a Hernández et al., (2014), precisa que “la investigación transversal recolecta datos en un solo momento, es como una retrato de lo que acontece” (p. 150).

3.2.2. Nivel de Investigación

La presente investigación fue de nivel correlacional; porque, estudiamos la relación entre las variables de estudio.

El enfoque que utilizamos en la investigación fue el cuantitativo y cualitativo para la recolección, procedimiento y análisis de la información; así como, para profundizar conocimientos teóricos.

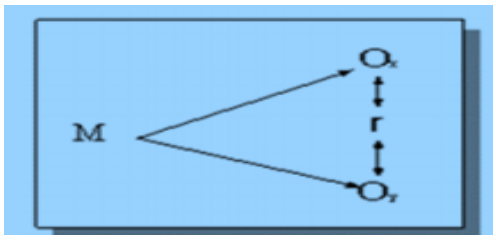
Para Hernández et al., (2014), el enfoque cuantitativo "utiliza la recolección de datos para probar hipótesis con base en la medición numérica y los análisis estadísticos" (p. 534).

3.3. Diseño de Investigación

El diseño de la investigación fue el diseño no experimental, debido a que no se manipuló ninguna de las variables de estudio, solo se observó en su estado natural.

Para Hernández, Fernández y Baptista (2010), "La investigación No experimental son estudios que se realizan sin la manipulación deliberada de las variables en estudio y en los que solo se observan los fenómenos en su ambiente natural para analizarlos" (p. 185).

Esquema de la investigación:



Dónde:

M = Personas bancarizadas entre 18 a 70.

Ox = Delito informático.

r = Relación existente entre las dos variables.

Oy = Operaciones financieras.

3.4. Población y Muestra

3.4.1. Población

Según García (2011) “la población es el conjunto mayor de objetos, que tienen al menos una característica común, cuyo estudio nos interesa o acerca de los cuales se desea información” (p. 56).

Para determinar la población, se tomó como fuente a Ipsos Perú (2021) que nos indica que más de 8.9 millones de peruanos están bancarizados lo que representa el 52% de la población de 40 a 70 años, del cual se tomó como población para la presente investigación a 836 bancarizados de entre 40 a 70 personas que radican en la provincia de Coronel Portillo, región de Ucayali, con el fin de realizar el presente estudio.

3.4.2. Muestra

Tamayo (2002), indica que “es el grupo de personas que se toma de la población, para investigar un fenómeno estadístico” (p. 363).

Fórmula:

$$n = \frac{NxZ^2xpxq}{e^2(N-1) + Z^2xpxq}$$

Dónde:

N = Población o Universo

Z = Nivel de confianza

e = Margen de error

p = Probabilidad de Éxito

q = Probabilidad de Fracaso

n = Muestra Inicial

Cálculo de la muestra

N = 836

Z = 1.96

e = 0.05

p = 0.50

q = 0.50

n = 263

Aplicando la fórmula del cálculo de la muestra se tuvo como resultado a 263 personas bancarizadas de entre 18 a 70 años a los cuales se aplicó el instrumento de investigación.

En conclusión la población y muestra de estudio quedó conformada de la siguiente manera:

Población : 836 personas de 40 a 70 años de edad.

Muestra : 263 personas de 40 a 70 años de edad.

3.5. Técnicas e Instrumentos de Recolección de Datos

3.5.1. Técnica

La técnica de investigación fue la encuesta dado que nos permitió obtener información de manera directa para posteriormente analizarlos mediante los objetivos

Gave et al., (2011), menciona que “la encuesta es una técnica consignada a obtener datos de varios individuos cuyas opiniones impersonales interesan al investigador, se utiliza un listado de preguntas escritas que se entregan a los sujetos, a fin de que las contesten igualmente por escrito (p. 80).

3.5.2. Instrumento

Para el proceso de recolección de datos utilizamos el cuestionario con la que obtuvimos los datos respecto a las variables de estudio.

3.6. Validación y Confiabilidad del Instrumento

La validación de los instrumentos se realizó mediante opinión de expertos, especialmente docentes de la Universidad Nacional de Ucayali y la confiablidad se realizó mediante sistema de SSPS.

3.7. Procedimiento de Recolección de Datos

Se procesaron los datos recolectados en tablas estadísticas, ya que, al ser una investigación cuantitativa se trabajó por porcentajes en la cual se siguió el siguiente procedimiento.

El primer paso, se inició buscando información bibliográfica para ampliar los conocimientos en cuanto a las variables de estudio.

El segundo paso, se procedió a elaborar los instrumentos de investigación.

El tercero paso se efectuó la aplicación del instrumento de investigación, Finalmente se realizó la prueba de hipótesis y planteamos la discusión, conclusiones y recomendaciones de la investigación.

Tabla 2

Categoría de análisis del coeficiente de correlación Rho de Spearman

Correlación	
Correlación positiva perfecta	+1
Correlación positiva muy fuerte	+0,90 a +0,99
Correlación positiva fuerte	+0,75 a +0,89
Correlación positiva media	+0,50 a +0,74
Correlación positiva débil	+0,25 a +0,49
Correlación positiva muy débil	+0,10 a +0,24
No existe correlación alguna	-0,09 a +0,09
Correlación negativa muy débil	-0,10 a -0,24
Correlación negativa débil	-0,25 a -0,49
Correlación negativa media	-0,50 a -0,74
Correlación negativa fuerte	-0,75a -0,89
Correlación negativa muy fuerte	-0,90 a -0,99
Correlación negativa perfecta	-1

Fuente: Gave et al., (2011).

3.8. Presentación de Datos

Los resultados obtenidos se muestran en figuras y tablas cada una de ellas analizadas de forma cuantitativa con el propósito de conocer la relación de las variables.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

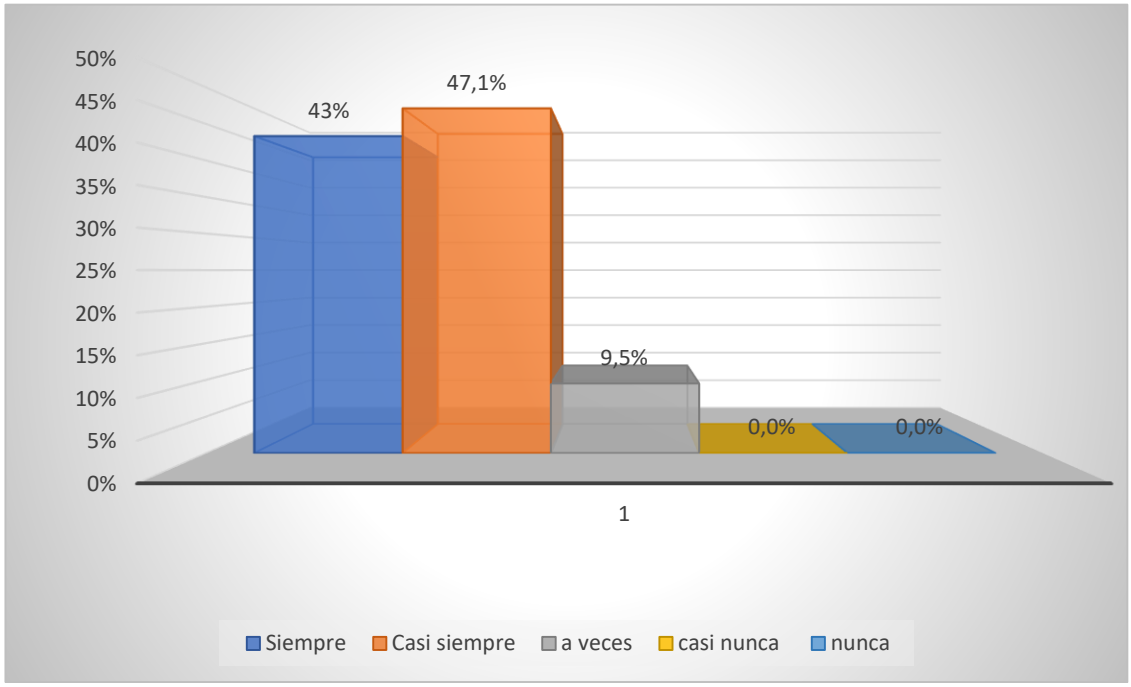
4.1. Descripción de Resultados

Variable X: Delito Informático

En la Figura 1**,** se observa que el 47.1% de los encuestados creen que casi siempre las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes, el 43% cree que siempre en las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes y el 9.5% cree que a veces las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes.

Figura 1

¿Cree usted que las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes?

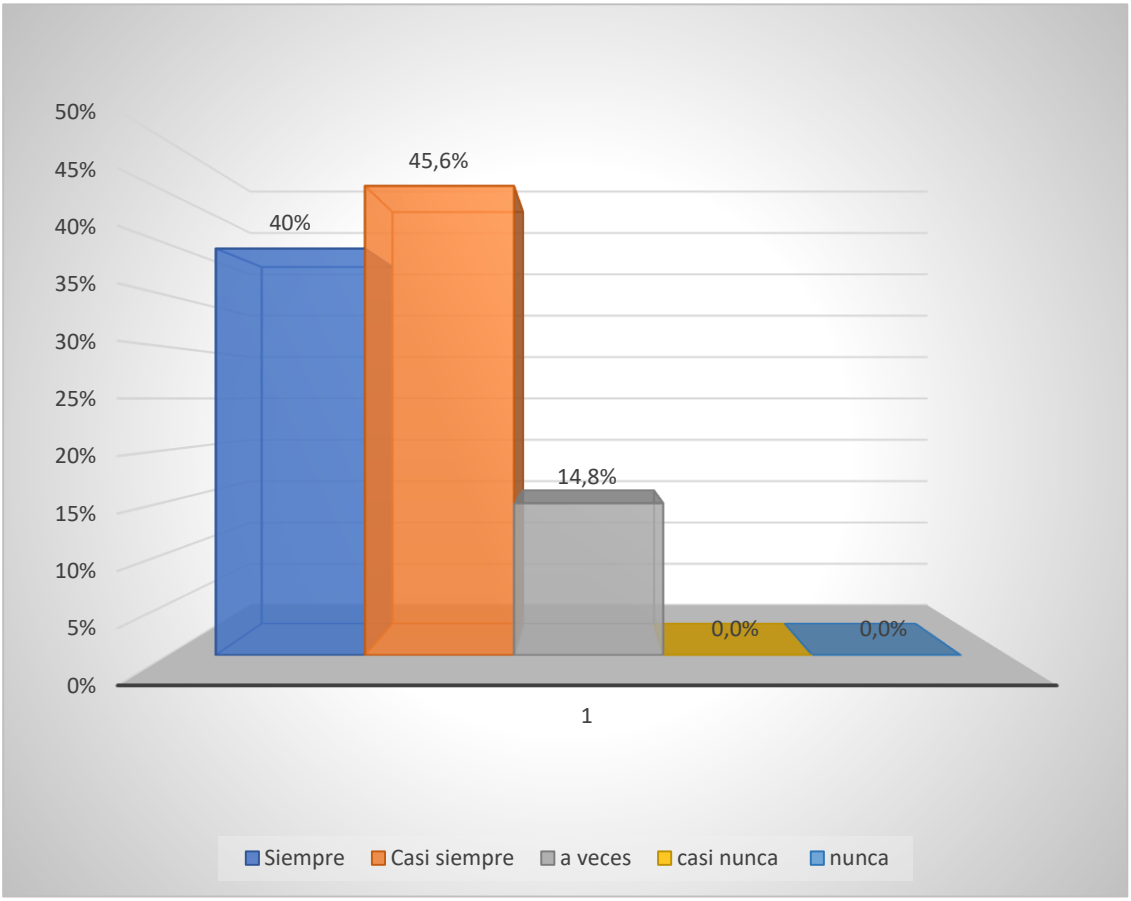


Fuente: Cuestionario.

En la Figura 2**,** se observa que 45.6% de los encuestados mencionaron que casi siempre se debería desarrollar políticas de protección de información en las instituciones bancarias, el 40% indicó que siempre se debería desarrollar políticas de protección de información en las instituciones bancarias y el 14.8% considera que a veces se debería desarrollar políticas de protección de información en las instituciones bancarias.

Figura 2

¿Considera que se debería desarrollar políticas de protección de información en las instituciones bancarias?

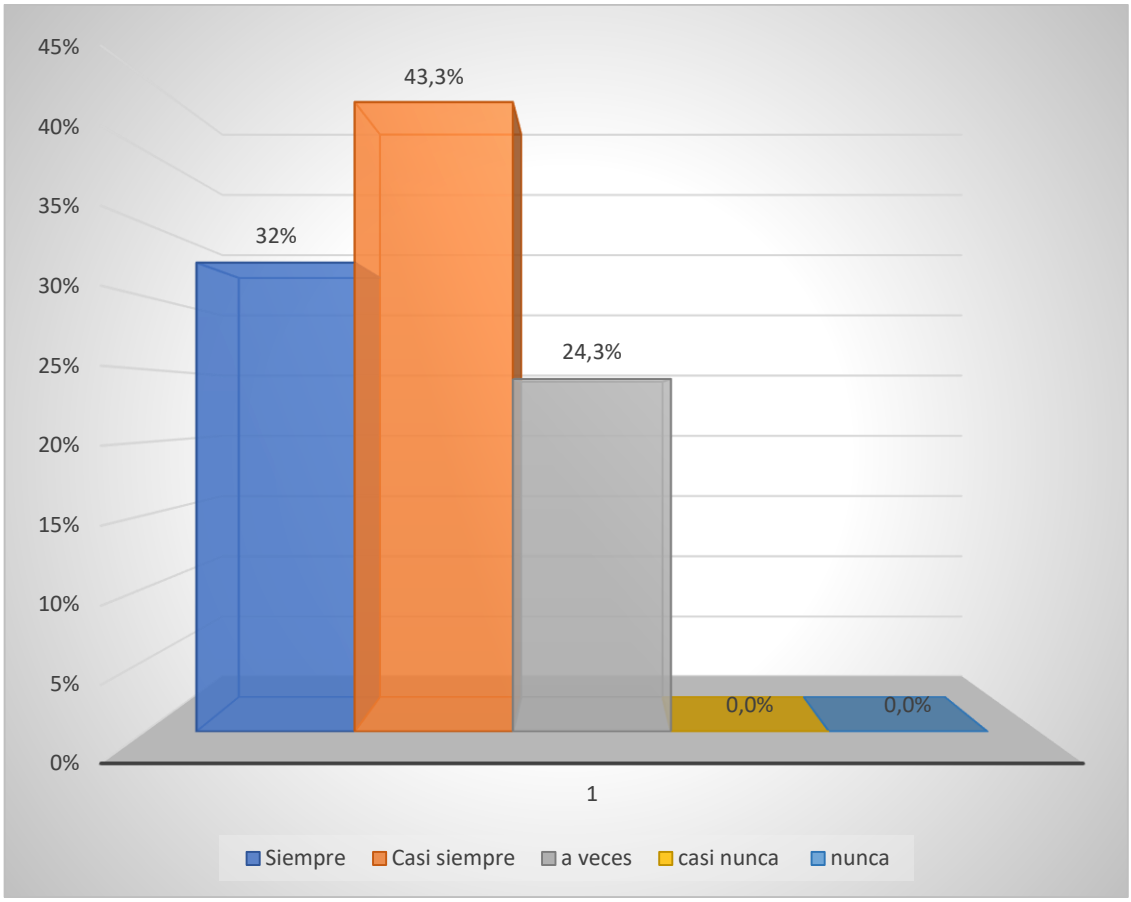


Fuente: Cuestionario.

En la Figura 3**,** se muestra que el 43.3% de los encuestados casi siempre sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores, el 32% considera que siempre sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores y el 24.3% a veces en sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores.

Figura 3

¿En algún momento sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores?



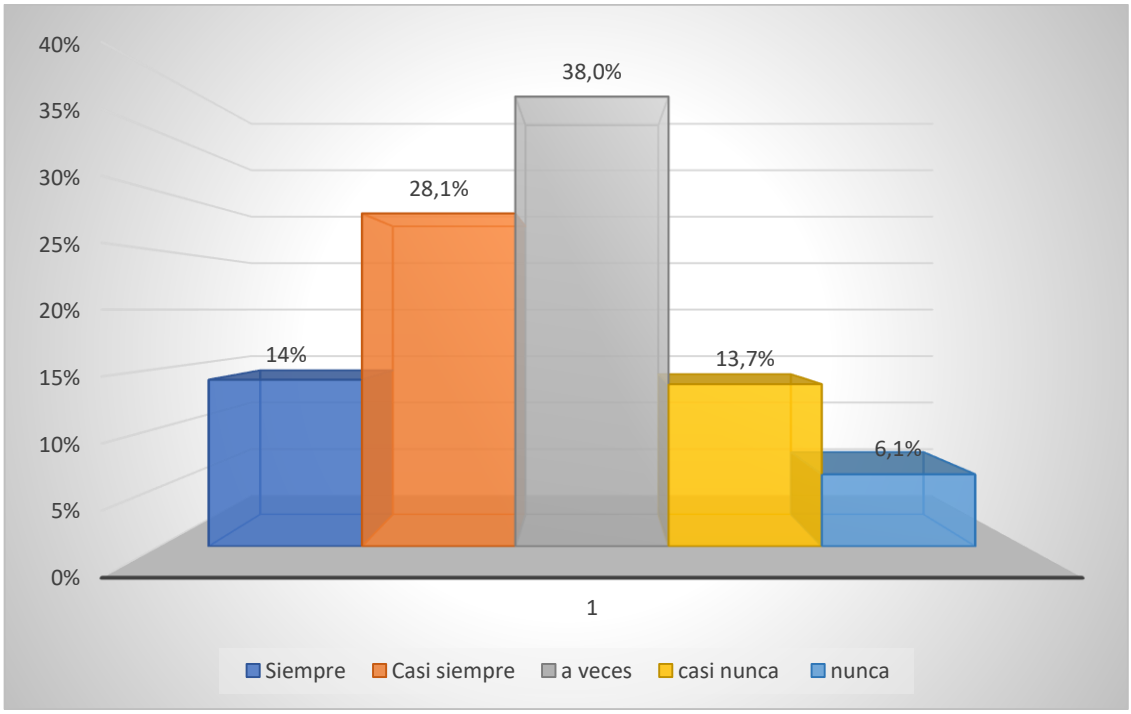
Fuente: Cuestionario.

Dimensión: Uso ilegal de la información

En la Figura 4, se muestra que el 38% de los encuestadas indicaron que a veces fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas, 28.1% casi siempre fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas, el 14% indicó que siempre fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas, el 13.7% casi nunca fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas y el 6.1 % nunca fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas.

Figura 4

¿Usted fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas?

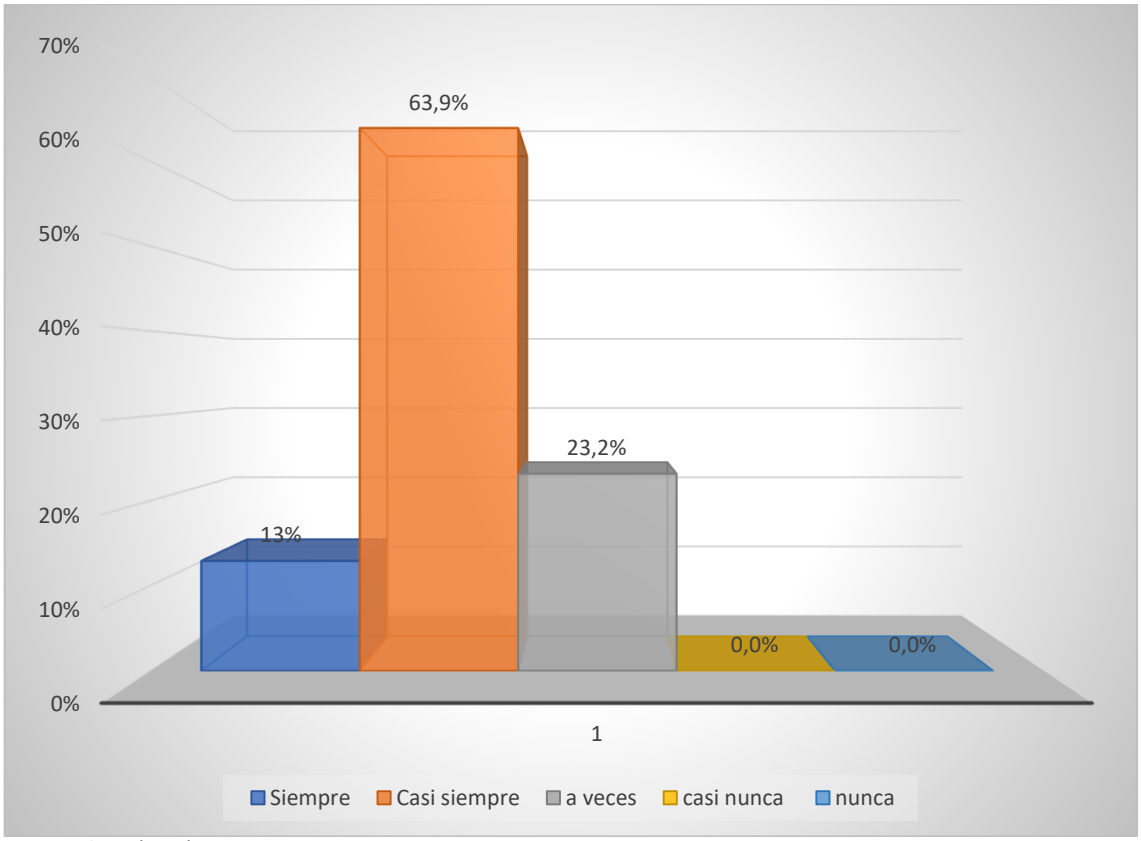


Fuente: Cuestionario.

En la Figura 5, muestra que el 63.9% de los encuestados consideró que casi siempre hicieron mal uso de su información personal las instituciones bancarias, 23.2% considero que a veces hicieron mal uso de su información personal las instituciones bancarias, el 13% considera que siempre hicieron mal uso de su información personal las instituciones bancarias.

Figura 5

¿Usted consideró que hicieron mal uso de su información personal las instituciones bancarias?

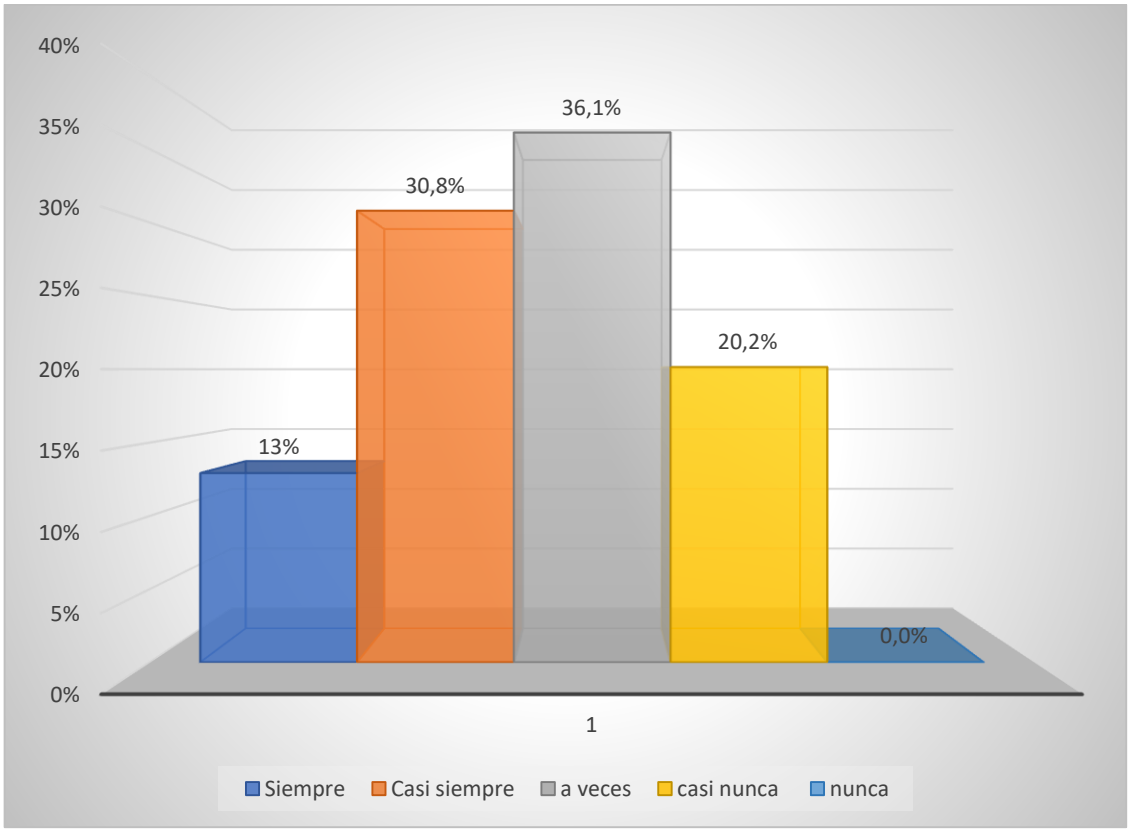


Fuente: Cuestionario.

En la Figura 6, se observa que el 36.1% de los encuestados a veces se siente vulnerable ante los estafadores por estar bancarizada, el 30.8% casi siempre se siente vulnerable ante los estafadores por estar bancarizada, el 13% siempre se siente vulnerable ante los estafadores por estar bancarizada y el 20.2% casi nunca se siente vulnerable ante los estafadores por estar bancarizada.

Figura 6

¿Se siente vulnerable ante los estafadores por estar bancarizada?



Fuente: Cuestionario.

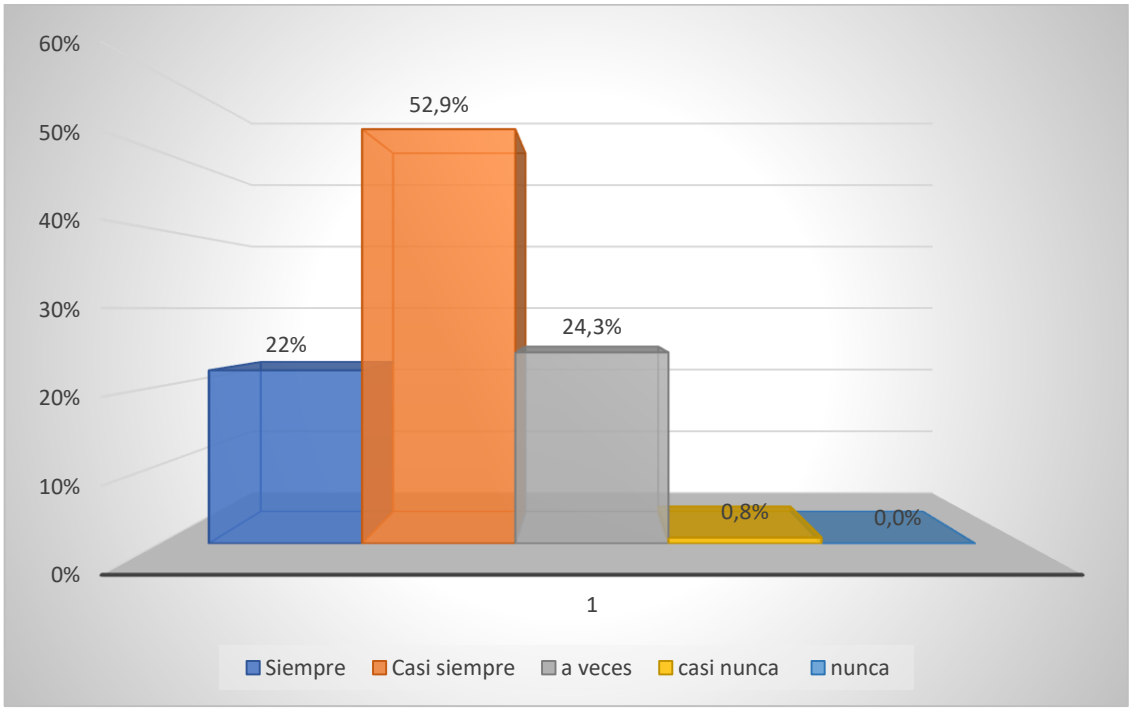
Variable Y: Operaciones Financieras

Dimensión: Operaciones Phishing

En la Figura 7**,** se observa 52.9% de los encuestados casi siempre llego a ser víctima en algún momento de robo por medios electrónicos, 24.3% a veces llego a ser víctima en algún momento de robo por medios electrónicos y el 22% considero que siempre llego a ser víctima en algún momento de robo por medios electrónicos.

Figura 7

¿Llegó a ser víctima en algún momento de robo por medios electrónicos?

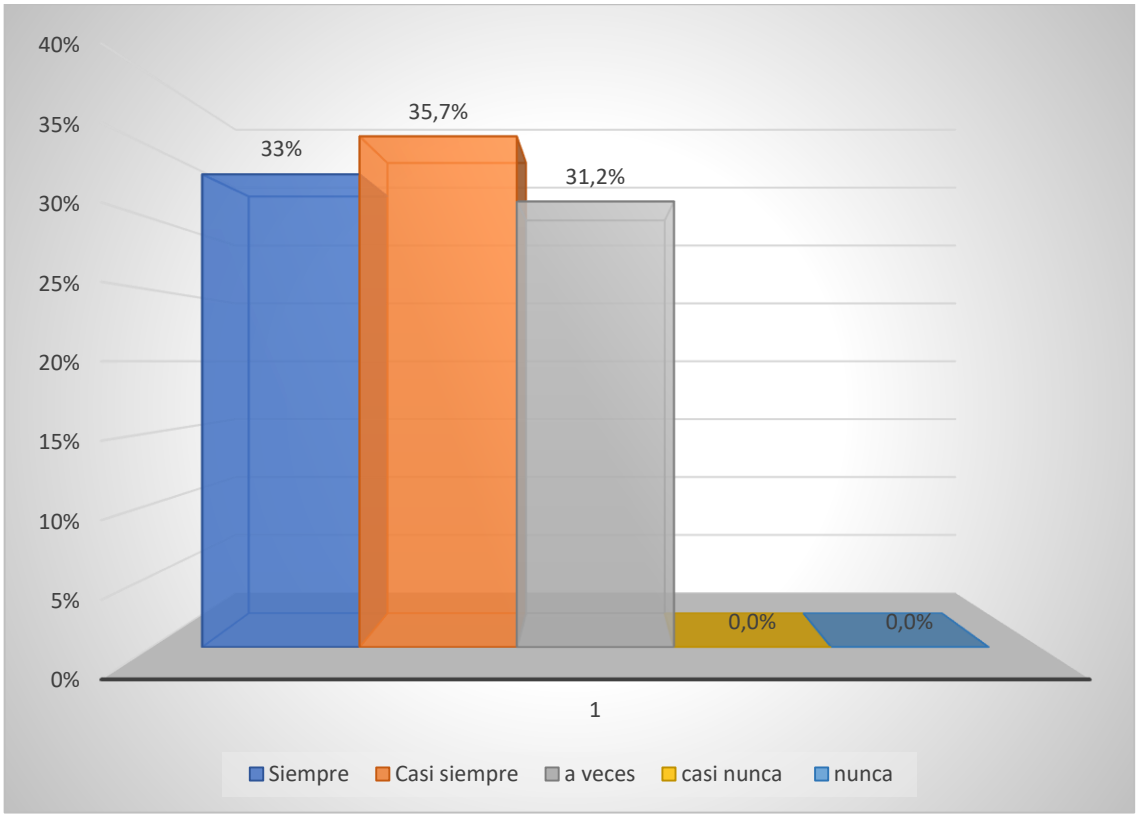


Fuente: Cuestionario.

En la Figura 8, se muestra que el 35.7% de los encuestados consideran que casi siempre que el uso de aplicativos bancarios lo hace más propenso hacia las estafas, 33% siempre considera que el uso de aplicativos bancarios lo hace más propenso hacia las estafas y el 31.2% a veces considera que el uso de aplicativos bancarios lo hace más propenso hacia las estafas.

Figura 8

¿Considera que el uso de aplicativos bancarios lo hace más propenso hacia las estafas?

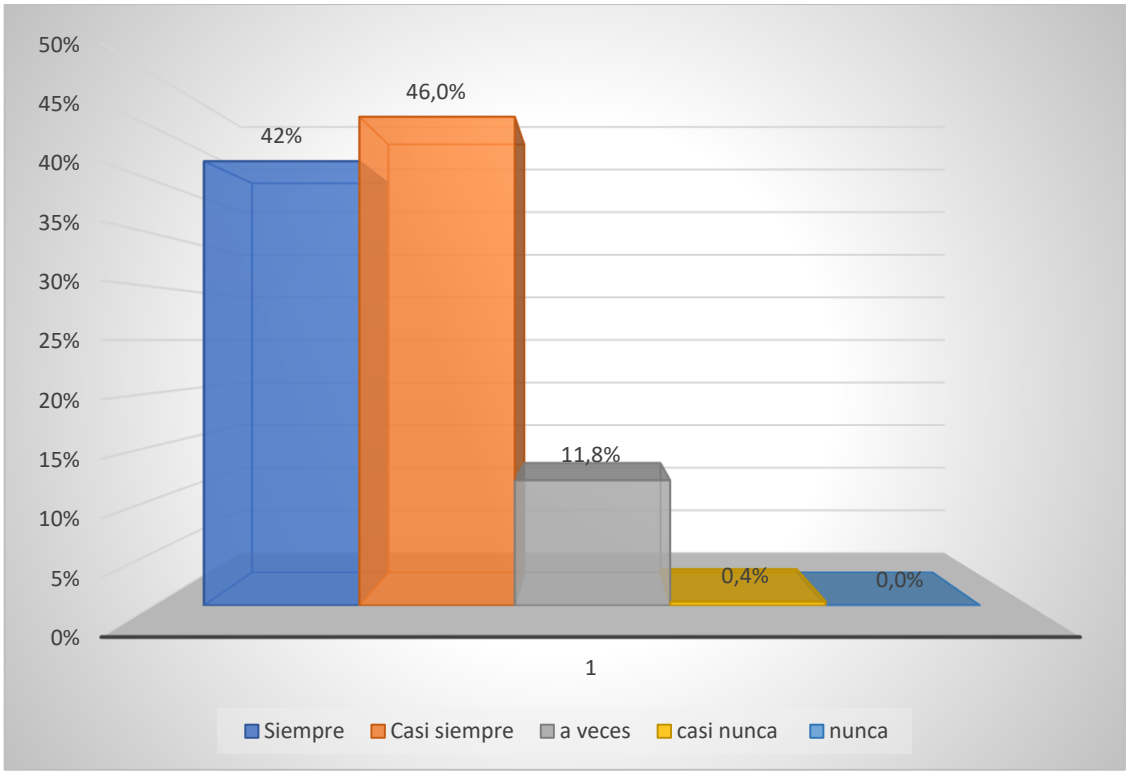


Fuente: Cuestionario.

En la Figura 9, se observa que el 46% de los encuestados casi siempre considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea, el 42% siempre considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea , el 11.8% a veces considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea y el 0.4% casi nunca considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea.

Figura 9

¿Considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea?



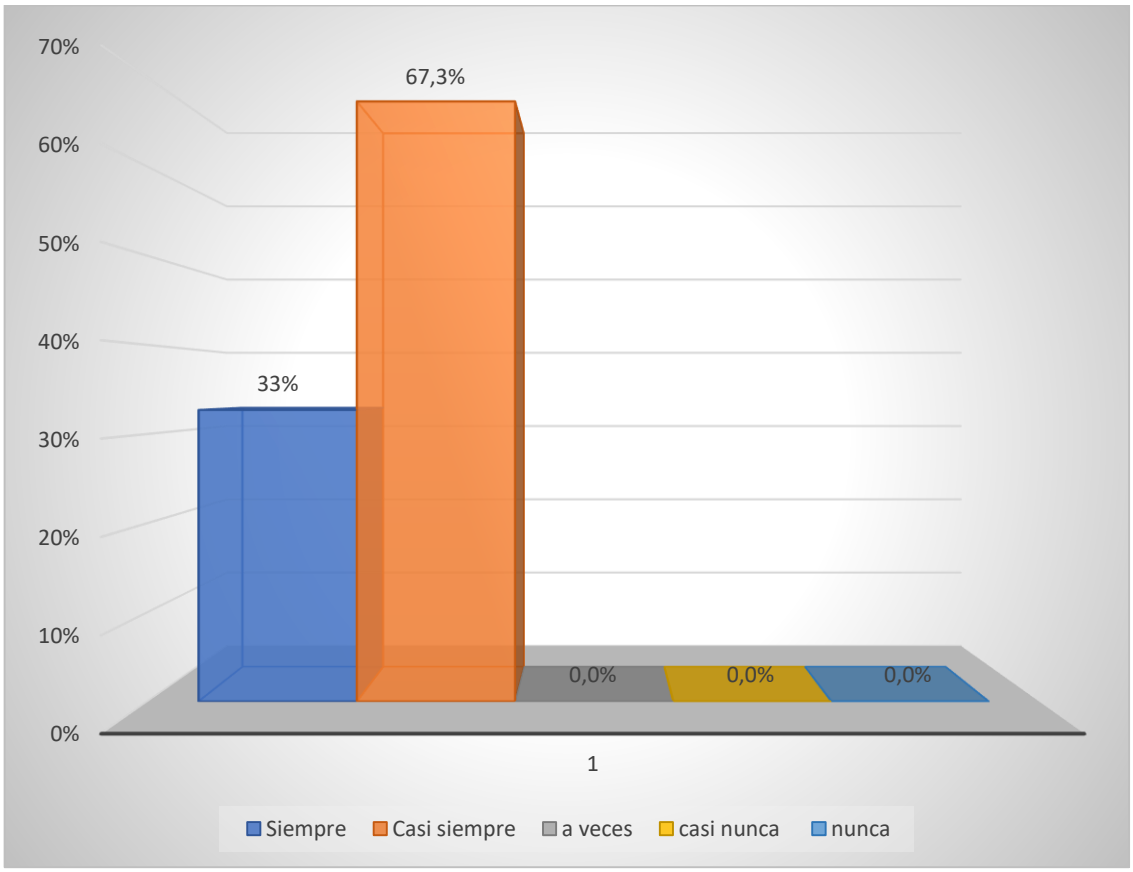
Fuente: Cuestionario.

Dimensión: Gestión de Riesgo

En la Figura 10, se observa que el 67.3% de los encuestados indican que casi siempre las instituciones bancarias deben desarrollar estrategias que cuiden a sus clientes ante posibles estafas o robos, el 33% mencionan que siempre las instituciones bancarias deben desarrollar estrategias que cuiden a sus clientes ante posibles estafas o robos.

Figura 10

¿Las instituciones bancarias deben desarrollar estrategias que cuiden a sus clientes ante posibles estafas o robos?

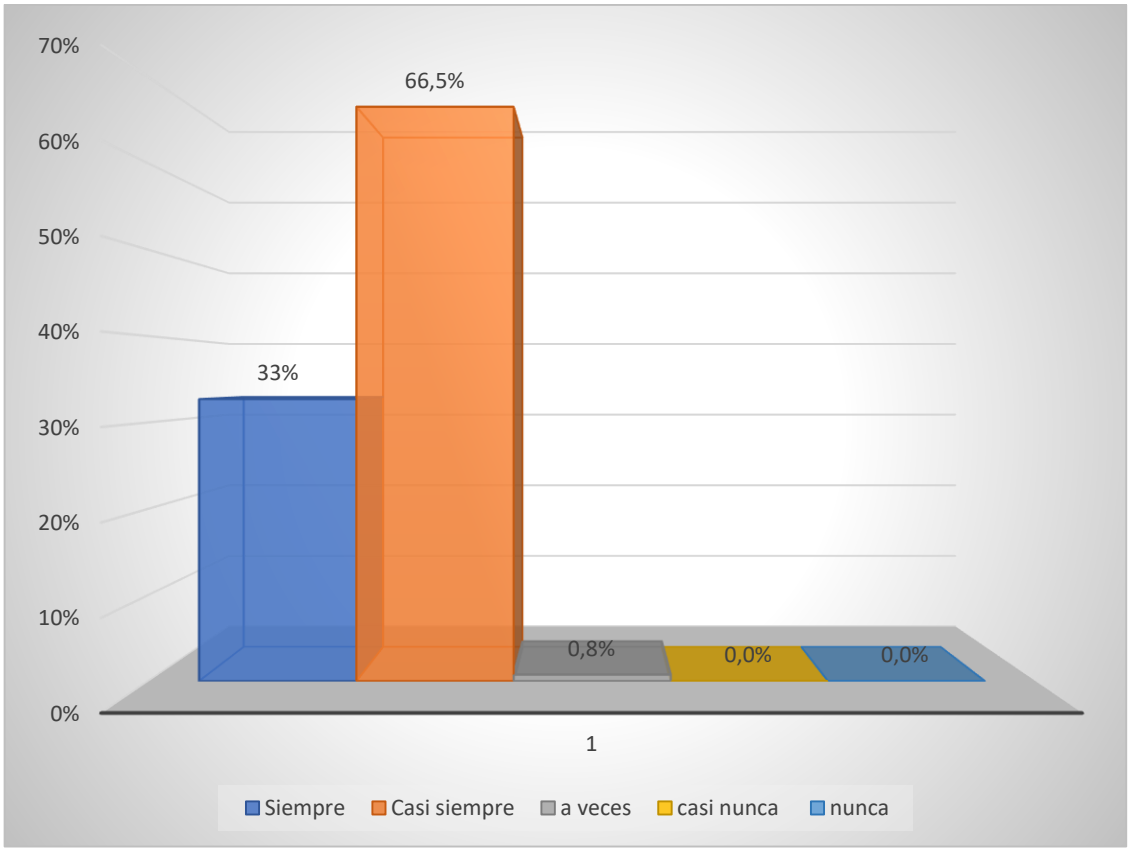


Fuente: Cuestionario.

En la Figura 11**,** muestra que el 66.5% de los encuestados considera que casi siempre se debería monitorear las operaciones sospechosas por las instituciones bancarias, 33% indicaron que siempre se debería monitorear las operaciones sospechosas por las instituciones bancarias y el 0.8% a veces se debería monitorear las operaciones sospechosas por las instituciones bancarias.

Figura 11

¿Considera que se debería monitorear las operaciones sospechosas por las instituciones bancarias?



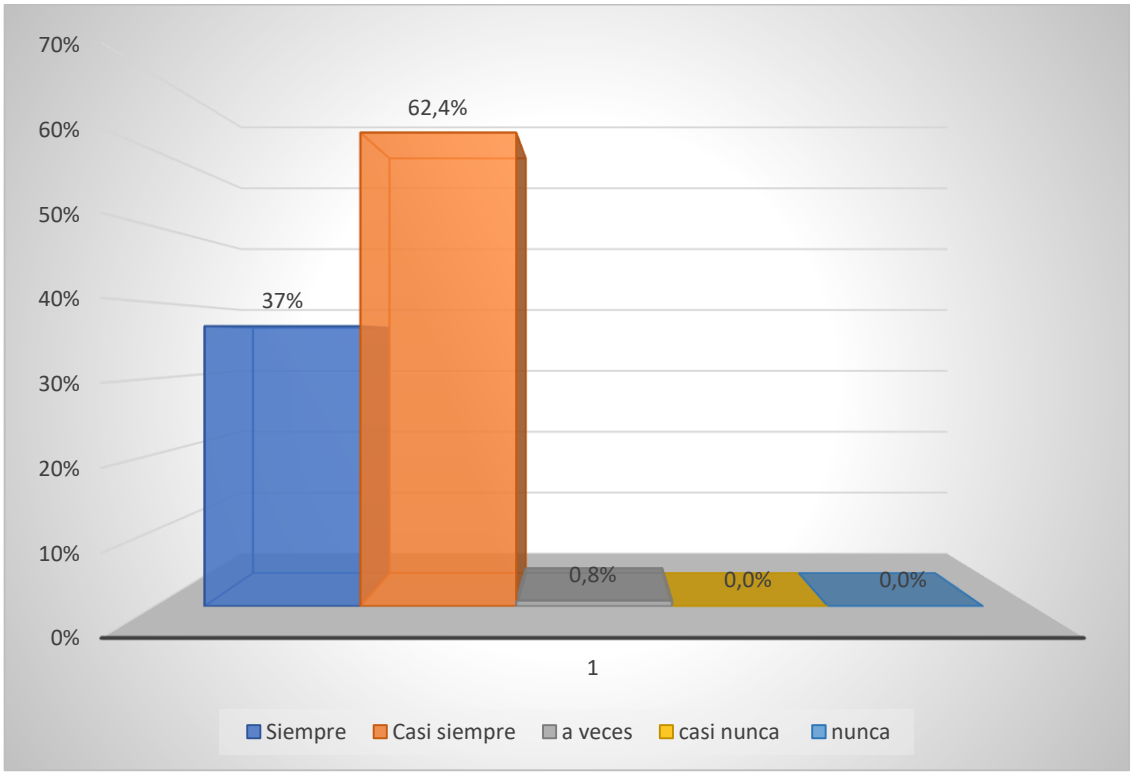
Fuente: Cuestionario.

Dimensión: Otorgamiento de Créditos

En la Figura 12, muestra que el 62.4% casi siempre cree instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional, el 37% siempre cree instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional y el 0.8% a veces cree instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional.

Figura 12

¿Cree instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional?

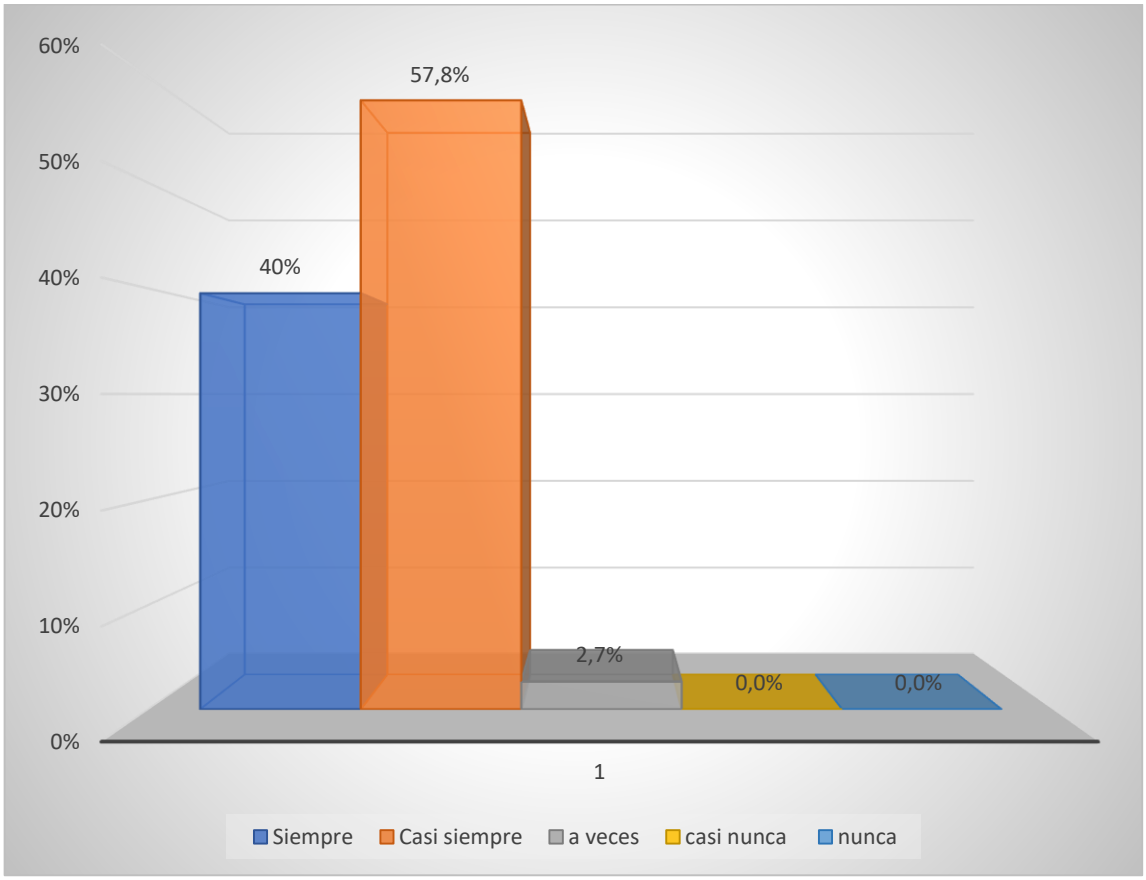


Fuente: Cuestionario.

En la Figura 13, se observa que el 57.8% indicaron que casi siempre las tarjetas de crédito deben contar con un seguro sin costos adicionales, 40% consideran que las tarjetas de crédito deben contar con un seguro sin costos adicionales y el 2.7% a veces consideran las tarjetas de crédito deben contar con un seguro sin costos adicionales.

Figura 13

¿Consideras que las tarjetas de crédito deben contar con un seguro sin costos adicionales?



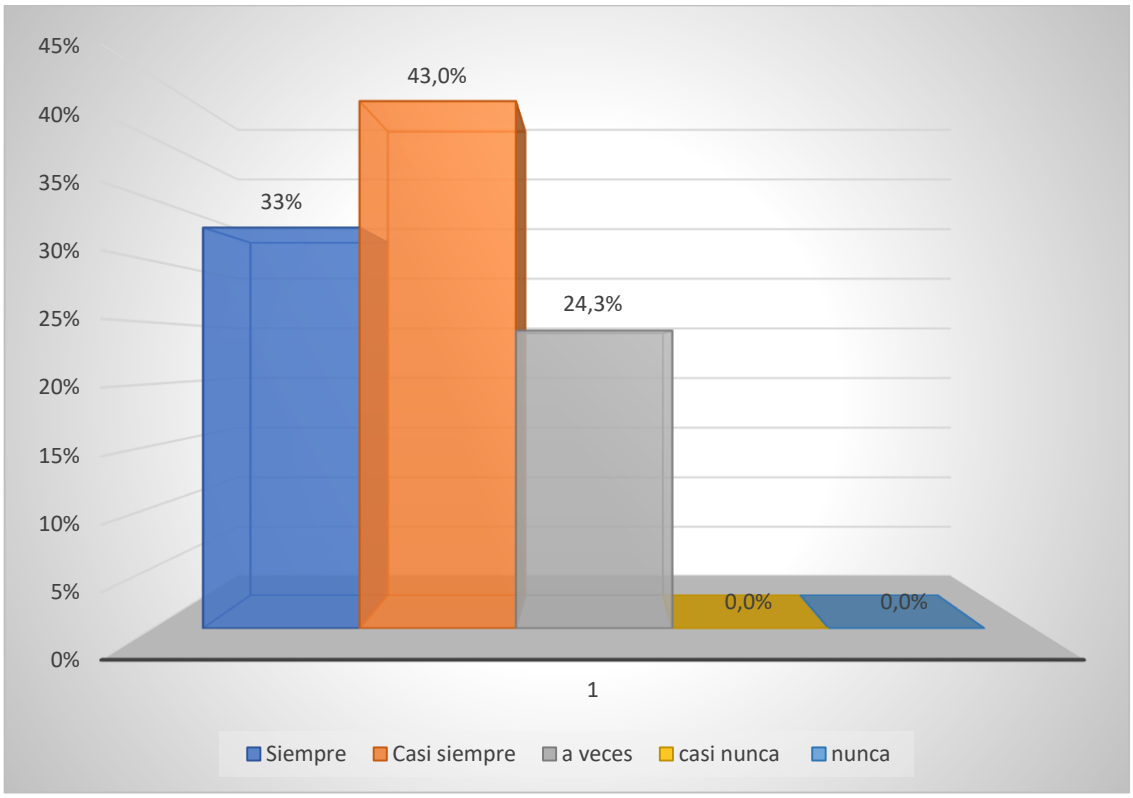
Fuente: Cuestionario.

+

En la Figura 14, se muestra que el 43% de los encuestados casi siempre cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas, el 33% siempre cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas y el 24.3% a veces cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas.

Figura 14

¿Cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas?



Fuente: Cuestionario.

4.2. Prueba de Hipótesis

4.2.1. Hipótesis General

- El delito informático incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022.

Paso 1: Planteamiento de la Hipótesis Nula e Hipótesis Alterna

- **Hipótesis nula (Ho):** El delito informático no incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022.

  (p=0)
- **Hipótesis alterna (Hi):** El delito informático incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022.

  - p > 0

Paso 2: Establecer el nivel de significación

- El nivel de significancia alfa α=0.05, para un nivel de confianza del 95%.

Paso 3: Selección del estadística de prueba

- El estadístico de prueba es el Rho de Spearman**.**

Paso 4: Reglas de la decisión

- Rechazar la Ho cuando la significancia de “p” valor < α (0.05) y aceptar la Ho cuando la significancia de “p” valor > α (0.05).

Paso 5: Cálculo

- Se utiliza el rho Spearman de una cola y se tuvo como resultado RHO= 756 y un p valor de 0.000 como se detalla en la Tabla 3.

Tabla 3

Prueba de correlación de Rho de Spearman de las variables delito informático y operaciones financieras

			Delito informático	Operaciones financieras
Rho de Spearman	Delito informático	Coeficiente de correlación	1,000	,756 **
		Sig. (unilateral)	.	,000
		N	263	263
	Operaciones financieras	Coeficiente de correlación	,756**	1,000
		Sig. (unilateral)	,000	.
		N	263	263

**. La correlación es significativa en el nivel 0,01 (1 cola).

Paso 5: Conclusión

- El grado de significancia del coeficiente de correlación de Rho Spearman es de p=0.000 siendo esta menos al α=0.05, por lo cual se permite rechazar la hipótesis nula y aceptar la alterna, donde precisa que el delito de información incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022, dado que el rho=756 correlación positiva fuerte.

4.2.2. Hipótesis Específica 1

- Existe incidencia entre el delito de información y las operaciones phishing en los bancos de la provincia de Coronel Portillo – Ucayali 2022.

Paso 1: Planteamiento de la Hipótesis Nula e Hipótesis Alterna

- **Hipótesis nula (Ho):** No existe incidencia entre el delito informático y las operaciones phishing en los bancos de la provincia de Coronel Portillo – Ucayali 2022.

  p=0
- **Hipótesis alterna (Hi):** Existe incidencia entre el delito informático y las operaciones phishing en los bancos de la provincia de Coronel Portillo – Ucayali 2022.

  - p > 0

Paso 2: Establecer el nivel de significación

- El nivel de significancia alfa α=0.05, para un nivel de confianza del 95%.

Paso 3: Selección del estadística de prueba

- El estadístico de prueba es el Rho de Spearman**.**

Paso 4: Reglas de la decisión

- Rechazar la Ho cuando la significancia de “p” valor < α (0.05) y aceptar la Ho cuando la significancia de “p” valor > α (0.05).

Paso 5: Cálculo

- Se utiliza el rho Spearman de una cola y se tuvo como resultado Rho= 553 y un p valor de 0.000 como se detalla en la Tabla 4.

Tabla 4

Prueba de correlación de Rho de Spearman entre de las variables delito informático y operaciones phishing

			Delito informático	Operaciones phishing
Rho de Spearman	Delito informático	Coeficiente de correlación	1,000	,553**
		Sig. (unilateral)	.	,000
		N	263	263
	Operaciones phishing	Coeficiente de correlación	,553**	1,000
		Sig. (unilateral)	,000	.
		N	263	263

**. La correlación es significativa en el nivel 0,01 (1 cola).

Paso 5: Conclusión y/o interpretación

- El grado de significancia del coeficiente de correlación de Rho Spearman es de p=0.000 siendo esta menos al α=0.05, por lo cual se permite rechazar la hipótesis nula y aceptar la alterna, lo que indica que existe incidencia entre el delito informático y las operaciones phishing en los bancos de la provincia de Coronel Portillo – Ucayali 2022, dado que el rho=553 correlación positiva media.

4.2.3. Hipótesis Específica 2

- Existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de Coronel Portillo – Ucayali 2022.

Paso 1: Planteamiento de la Hipótesis Nula e Hipótesis Alterna

- **Hipótesis nula (Ho):** No existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de Coronel Portillo – Ucayali 2022.

  - p=0

- **Hipótesis alterna (Hi):** Existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de Coronel Portillo – Ucayali 2022.

  - p > 0

Paso 2: Establecer el nivel de significación

- El nivel de significancia alfa α=0.05, para un nivel de confianza del 95%.

Paso 3: Selección del estadística de prueba

- El estadístico de prueba es el Rho de Spearman**.**

Paso 4: Reglas de la decisión

- Rechazar la Ho cuando la significancia de “p” valor < α (0.05) y aceptar la Ho cuando la significancia de “p” valor > α (0.05).

Paso 5: Cálculo

- Se utiliza el rho Spearman de una cola y se tuvo como resultado Rho= 685 y un p valor de 0.000 como se detalla en la Tabla 5.

Tabla 5

Prueba de correlación de Rho de Spearman entre las variables Factores educativos y gestión de riesgo

			Delito informático	Gestión de riesgo
Rho de Spearman	**Delito informático**	Coeficiente de correlación	1,000	,685*
		Sig. (unilateral)	.	,000
		N	263	263
	Gestión de riesgo	Coeficiente de correlación	,685*	1,000
		Sig. (unilateral)	,000	.
		N	263	263

**. La correlación es significativa en el nivel 0,01 (1 cola).

Paso 5: Conclusión

- El grado de significancia del coeficiente de correlación de Rho Spearman es de p=0.000 siendo esta menos al α=0.05, por lo cual se permite rechazar la hipótesis nula y aceptar la alterna, lo que indica que existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de Coronel Portillo – Ucayali 2022, dado que el rho=685 correlación positiva media.

4.2.4. Hipótesis Específica 3

- Existe incidencia entre el delito informático y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022.

Paso 1: Planteamiento de la Hipótesis Nula e Hipótesis Alterna

- **Hipótesis nula (Ho):** No existe incidencia entre el delito informático y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022.

  p=0
- **Hipótesis alterna (Hi):** Existe incidencia entre el delito informático y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022.

  - p > 0

Paso 2: Establecer el nivel de significación

- El nivel de significancia alfa α=0.05, para un nivel de confianza del 95%.

Paso 3: Selección de la estadística de prueba

- El estadístico de prueba es el Rho de Spearman**.**

Paso 4: Reglas de la decisión

- Rechazar la Ho cuando la significancia de “p” valor < α (0.05) y aceptar la Ho cuando la significancia de “p” valor > α (0.05).

Paso 5: Cálculo

- Se utiliza el Rho Spearman de una cola y se tuvo como resultado Rho= 850 y un p valor de 0.000 como se detalla en la Tabla 6.

Tabla 6

Prueba de correlación de Rho de Spearman entre las variables Factores social y otorgamiento de crédito

			Delito informático	Otorgamiento de crédito
Rho de Spearman	Delito informático	Coeficiente de correlación	1,000	,850**
		Sig. (unilateral)	.	,000
		N	263	263
	Otorgamiento de crédito	Coeficiente de correlación	,850**	1,000
		Sig. (unilateral)	,000	.
		N	263	263

**. La correlación es significativa en el nivel 0,01 (1 cola).

Paso 5: Conclusión

- El grado de significancia del coeficiente de correlación de Rho Spearman es de p=0.000 siendo esta menos al α=0.05, por lo cual se indica que existe incidencia entre el delito informático y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022, dado que el rho=685 correlación positiva fuerte.

4.3. Discusión de Resultados

Se expone los resultados obtenidos durante el proceso de investigación los cuales nos permitieron contrastar las hipótesis de la investigación y constatar el logro de los objetivos establecidos, dado que el objetivo general de la investigación fue Determinar como el delito informático incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022, contrastando la relación entre el delito informático y las operaciones financieras, ya que se obtuvo un Rho de Spearman nos dio como resultado rho=0.756 y un p=0.000 lo muestra que existe una correlación positiva fuerte.

Chiluisa (2021), en su estudio titulado “Los delitos informáticos y los vacíos legales que afectan a los ciudadanos” Universidad Católica de Santiago de Guayaquil” en la cual tuvo como resultado que la mayor parte de la población hoy en día maneja las herramientas tecnológicas y es el medio en la cual se vulnera la información de las personas siendo más accesibles para los delincuentes cibernéticos cometiendo diversos delitos que quedan impunes, por su parte, Morán y Morán (2020), en su estudio titulado “Delitos informáticos, reforma al artículo 190 ce COIP en el contexto de la emergencia sanitaria Ecuador 2020”, Universidad de Guayaquil – Ecuador, tuvo como resultado que los delitos informáticos están evolucionado constantemente por lo que es necesario tipificar los actos delictivos y revisar periódicamente los nuevos delitos informáticos para poder sancionarlas.

Por su parte, Mori (2019) en su estudio titulado “Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, Periodo 2008 al 2012” tuvo como resultado que se encontró que los jueces aceptan que existe ausencia de formación tecnológica en el delito informático pero los fiscales y

policías dicen estar en desacuerdo, que la deontología tecnológica que afecta la competitividad de los operadores de justicia influye en la impropia determinación del tipo penal y en la competitividad en la investigación y juzgamiento de los delitos informáticos obteniendo, Así mismo, De La Cruz (2021), en su estudio titulado “Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la Provincia de Huaura - Huacho 2018, tuvo los siguientes resultados el sistema financiero y bancario frente a los fraudes, no brinda garantía a sus clientes en los tiempos actual, además los clientes consideran que frente a las transacciones fraudulentas debe ser el sistema bancario y financiero quien debe responder a favor de sus clientes, aun cuando el cliente no contrate un seguro.

De la misma manera, Marín y Santa María (2021), en su estudio titulada “El ciberdelito de redes delictivas a escala global a entidades gubernamentales y la responsabilidad del órgano de control interno en una municipalidad de la región de Ucayali, año 2020”, tuvo como resultado que hay una estrecha relación entre los riesgos tecnológicos y la implementación de un área de prevención con un auditorio interno antifraude de los fondos de las municipalidades distritales o Provinciales, Posterior a la comprobación de los resultados podemos afirmar que el presente estudio existe relación entre el delito informático y las operaciones financieras.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se determinó que el delito informático incide significativamente en las operaciones financieras en los bancos de la provincia de Coronel Portillo-Ucayali 2022, dado que el nivel de significancia es de p=0.000 y el coeficiente Rho de Spearman tiene un valor de 756 por lo que se rechaza la hipótesis nula y se demuestra que existe correlación positiva fuerte entre el delito informático y las operaciones financieras.

- Se determinó que existe incidencia entre el delito informático y las operaciones phishing en los bancos de la provincia de Coronel Portillo – Ucayali 2022, dado que el nivel de significancia es de p=0.000 y el coeficiente Rho de Spearman tiene un valor de 553 por lo cual se rechaza la hipótesis nula y se demuestra que existe correlación positiva medio entre el delito informático y las operaciones phishing.

- Se determinó que existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de Coronel Portillo - Ucayali 2022, dado que el nivel de significancia es de p=0.000 y el coeficiente Rho de Spearman tiene un valor de 685 por lo que se rechaza la hipótesis nula y se demuestra que existe correlación positiva fuerte entre el delito informático y las gestión de riesgos.

- Se determinó que existe incidencia entre el delito informático y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022, dado que el nivel de significancia es de p=0.000 y el coeficiente Rho de Spearman tiene un valor de 850 por lo que se rechaza la hipótesis nula y se demuestra que existe correlación positiva fuerte entre el delito informático y el otorgamiento de créditos.

5.2. Recomendaciones

- Se recomienda a las entidades encargadas de supervisar a las instituciones financieras implementar políticas de gestión que garanticen a los clientes la seguridad en cuanto a efectuar operación, ya sean en ventanilla como haciendo uso de los medios tecnológicos.

- Así mismo se recomienda a las instituciones bancarias que deben monitorear de manera permanente las operaciones sospechosas para garantizar la seguridad que requieren los clientes y desarrollar medidas de seguridad efectivas con el fin de prevenir los fraudes electrónicos.

- También es necesario que las instituciones financieras informen de manera permanente a sus clientes sobre las medidas de seguridad que deben seguir para evitar ser víctimas de posibles fraudes cibernéticos para que estos sientan la confianza de efectuar sus operaciones en línea sin ningún temor garantizando el bienestar de los mismos.

- A los clientes de las instituciones bancarias de la provincia de Coronel Portillo deben tomar todas las medidas de seguridad si van a efectuar operaciones de manera virtual o presencial para no ser víctimas de la delincuencia, siguiendo las recomendaciones de los colaboradores de las instituciones bancarias les proporcionen.

REFERENCIAS BIBLIOGRÁFICAS

Alarcón Araiza, D. A. y Barrera Barón, J. A. (2017). Uso de internet y delito informático en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, sede Seccional Sogamoso 2016. Escuela de Posgrado. Lima, Perú, Universidad Norbert Wiener. Recuperado de: https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/1630/MAESTRO%20-%20%20Barrera%20Bar%c3%b3n%2c%20Javier%20Antonio.pdf?sequence=1&isAllowed=y

Ander – Egg, E. (1995). Técnicas de investigación social. 24a edición, Buenos Aires. Recuperado de: https://epiprimero.files.wordpress.com/2012/01/ander-egg-tecnicas-de-investigacion-social.pdf

Andina, A. A. (2022). Conoce las modalidades más comunes de delitos informáticos y cómo denunciarlos en el Perú. Andina. Obtenido de: https://andina.pe/agencia/noticia-conoce-las-modalidades-mas-comunes-delitos-informaticos-y-como-denunciarlos-el-peru-901507.aspx

Arteaga Poccori, V. y Choquehuanca Catari, N. (2017). Los factores perceptuales y su relación con la utilización del servicio de banca móvil en Arequipa Metropolitana – 2016. Universidad Nacional de San Agustín de Arequipa – Perú. Recuperado de: http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/2574/BSarpov.pdf?sequence=1&isAllowed=y

Belcic, I. (02 de 05 de 2020). Obtenido de https://www.avast.com/es-es/c-phishing

Blossiers Mazzini, C. M. (2018). Metodología de la investigación científica. Pautas metodológicas para elaborar un proyecto de investigación.

Costa Cevallos, M. A. y Ruíz Cruz, C. A. (2016). Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos. Universidad Nacional de Loja – Ecuador.

Chiluisa Mullo, D. O. (2021). “Los delitos informáticos y los vacíos legales que afectan a los ciudadanos”. Ecuador. Recuperado de: http://repositorio.ucsg.edu.ec/bitstream/3317/16501/1/T-UCSG-PRE-JUR-DER-MD-334.pdf

De La Cruz Sánchez, D. A. (2021). Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la provincia de Huaura - Huacho 2018. Universidad José Faustino Sánchez Carrión- Perú. Recuperado de: https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/4960/DIEGO%20ALBERTO%20DE%20LA%20CRUZ%20S%C3%81NCHEZ.pdf?sequence=1&isAllowed=y

Durán & Durán (2023). Delitos informáticos. Recuperado de: https://duranyduranabogadospenalistas.com/delitos-informaticos

García Oré, C. (2011). Estadística Descriptiva y Probabilidades para Ingenieros. Recuperado de: https://ebooks.arnoia.com/media/eb_0104/samples/9786123040277cap1-02.pdf

Hancco Zapana, E. Y. (2017). La tipificación de bien Jurídico Protegido en la Estructura del tipo penal Informático como causar de su deficiente regulación en la Ley 30096, Perú -2017. Recuperado de:

https://1library.co/document/zx50734q-tipificacion-juridico-protegido-estructura-informatico-causas-deficiente-regulacion.html

Hernández et al., (2014). Metodología de la investigación. México: McGraw Hill. 6ta. edición.

Hernández, S.; Fernández, C. y Baptista, L. (2010). Metodología de la investigación. Colombia: Editorial Mc Graw Hill.

Ipsos Perú (2021). Bancarización 2021. Recuperado de: https://www.ipsos.com/es-pe/bancarizacion-2021

López, J. F. (2020). Obtenido de https://economipedia.com/definiciones/operacion-financiera.html

Ley Nº 30096. Ley de Delitos Informáticos. Recuperado de: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Marín Ampuero, A. C. y Santa María Flores, E. (2021). El ciberdelito de redes delictivas a escala global a entidades gubernamentales y la responsabilidad del órgano de control interno en una municipalidad de la región de Ucayali, año 2020*"*. Universidad Nacional de Ucayali – Perú. http://repositorio.unu.edu.pe/bitstream/handle/UNU/5184/B02_2022_UNU_CONTABILIDAD_T_2021_ALEXIS-MARIN_ESTEFANY-SANTAMARIA.pdf?sequence=1&isAllowed=y

Morán Cevallos, J. D. y Morán Cevallos, R. N. (2020). "Delitos informáticos, reforma al artículo 190 ce COIP en el contexto de la Emergencia Sanitaria Ecuador 2020", Universidad de Guayaquil – Ecuador. Recuperado de: http://repositorio.ug.edu.ec/bitstream/redug/50908/1/Jonathan%20Mor%C3%A1n%20-%20Ruth%20Mor%C3%A1n%20BDER-TPrG%20227-2020.pdf

Mori Quiroz, F. (2019). Los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, Periodo 2008 al 2012. Universidad Nacional Federico Villarreal, Perú.

Gave Chagua, J. L.; Ramírez Rosales, F. G. Oseda Gago, D. y Gonzales Castro, A. (2011). ¿Cómo aprender y enseñar investigación científica? Editorial Universidad Nacional de Huancavelica. UNH. 1ª edición.

Paucar Rojas, E. (2020). Metodología y tesis cazando ideas. Editores Gamarra. 1ª. Edición.

Perú. (05 de 09 de 2022). Infobae. Obtenido de: https://www.infobae.com/america/peru/2022/09/05/delitos-informaticos-se-han-incrementado-en-el-peru/

Tamayo y Tamayo, M. (2002). Técnicas de investigación. 4ª edición. México: Editorial Mc Graw Hill.

Vilca Aira, G. L. (2018). Los hackers: delitos informáticos frente al código penal peruano. Facultad de Derecho y Ciencias Políticas. Anchas, Perú. Universidad Nacional Santiago Antúnez de Mayolo. Recuperado de: http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2496/T033_47272593_T.pdf?sequence=1&isAllowed=y

ANEXO

ANEXO 1: MATRIZ DE CONSISTENCIA

TÍTULO: "EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO - UCAYALI 2022"

<table>
<tr><th>PROBLEMAS</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES</th><th>DIMENSIONES</th><th>INDICADORES</th><th>METODOLOGÍA</th></tr>
<tr><td>Problema General</td><td>Objetivo General</td><td>Hipótesis General</td><td rowspan="3">DELITO INFORMÁTICO</td><td rowspan="2">X1: Acceso a una base de datos</td><td>X1.1 Vulnerabilidad de los datos</td><td rowspan="6">• Sistema de métodos
Método general: Inductivo - deductivo
• Tipo de investigación: Básica
En el tiempo: Transversal.
Nivel de la investigación: Correlacional
Diseño de la investigación: No Experimental
Enfoque de la investigación: cuantitativa
• Población y muestra
Población: 836 personas bancarizadas de 18 a 70 años
Muestra: 263
• Técnicas
Encuesta
• Instrumentos
Cuestionario.
• Técnicas de procesamiento de datos:
Se procedió a analizar los datos mediante EXCEL, los resultados se analizaron vía estadística descriptiva y para el contraste de hipótesis se utilizó el SPSS versión 21 y se seguirán 5 pasos.</td></tr>
<tr><td rowspan="2">¿De qué manera el delito informático incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo – Ucayali 2022?</td><td rowspan="2">Determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de Coronel Portillo - Ucayali 2022.</td><td rowspan="2">El delito de información incide significativamente en las operaciones facinerosas en los bancos de la provincia de Coronel Portillo - Ucayali 2022.</td><td>X1.2. vulnerabilidad de la información personal</td></tr>
<tr><td>X2: Uso ilegal de la información</td><td>X2.1. Suplantación</td></tr>
<tr><td>Problemas Específicos</td><td>Objetivos Específicos</td><td>Hipótesis Especificas</td><td rowspan="4">OPERACIONES FIANCIERAS</td><td rowspan="2">Y1: Operaciones Phishing</td><td rowspan="2">Y1.1. Captación mediante internet</td></tr>
<tr><td>¿En qué medida el delito informático incide en las operación phishing de los bancos en la provincia de Coronel Portillo - Ucayali 2022?</td><td>Determinar en qué medida el delito informático incide en las operaciones Phishing de los bancos en la provincia de Coronel Portillo - Ucayali 2022.</td><td>Existe incidencia entre el delito de información y las operaciones phishing de los bancos en la provincia de Coronel Portillo – Ucayali 2022.</td></tr>
<tr><td>¿En qué medida el delito informático se relaciona con la gestión de riesgos de los bancos de la provincia de Coronel Portillo – Ucayali 2022?</td><td>Determinar en qué mediada el delito informático tiene relación con la gestión de riesgos de los bancos de la provincia de Coronel Portillo - Ucayali 2022.</td><td>Existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de Coronel Portillo - Ucayali 2022.</td><td>Y2: Gestión de riesgos</td><td>Y2.1.Monitoreo de procesos
Y2.2. Estrategias de control</td></tr>
<tr><td>¿en qué medida el delito informático incide en la vulnerabilidad de los créditos otorgados por los bancos de la provincia de Coronel Portillo - Ucayali 2022?</td><td>Determinar en qué media el delito informático incide en vulnerabilidad de los créditos otorgados por los bancos de la provincia de Coronel Portillo - Ucayali 2022.</td><td>Existe incidencia entre el delito de información y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de Coronel Portillo – Ucayali 2022.</td><td>Y3: Otorgamiento de Créditos</td><td>Y3.1. Desembolsos de prestamos
Y3.2. Otorgamientos de tarjetas de crédito</td></tr>
</table>

ANEXO 1: MATRIZ DE INSTRUMENTOS

VARIABLE DE ESTUDIO	DIMENSIONES	INDICADORES	ÍTEMS
VARIABLE X DELITO INFORMÁTICO	**X1:** Acceso a una base de datos	**X1.1** Vulnerabilidad de los datos **X1.2.** Vulnerabilidad de la información personal	1. ¿Cree usted que las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes? 2. ¿Considera que se debería desarrollar políticas de protección de información en las instituciones bancarias? 3. ¿En algún momento sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores?
	X2: Uso ilegal de la información	**X2.1**. Suplantación	4. ¿Usted fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas? 5. ¿Usted consideró que hicieron mal uso de su información personal las instituciones bancarias? 6. ¿Se siente vulnerable ante los estafadores por estar bancarizada?
VARIABLE Y OPERACIONES FINANCIERAS	**Y1:** Operaciones Phishing	**Y1.1.** Captación mediante internet	7. ¿Llegó a ser víctima en algún momento de robo por medios electrónicos? 8. ¿Considera que el uso de aplicativos bancarios lo hace más propenso hacia las estafas? 9. ¿Considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea?
	Y2: Gestión de riesgos	**Y2.1**.Monitoreo de procesos **Y2.2.** Estrategias de control	10. ¿Las instituciones bancarias deben desarrollar estrategias que cuiden a sus clientes ante posibles estafas o robos? 11. ¿Considera que se debería monitorear las operaciones sospechosas por las instituciones bancarias?
	Y3: Otorgamiento de Créditos	**Y3.1.** Desembolsos de préstamos **Y3.2.** Otorgamientos de tarjetas de crédito	12. ¿Cree usted que las instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional? 13. ¿Consideras que las tarjetas de crédito deben contar con un seguro sin costos adicionales? 14. ¿Cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas?

ANEXO 2: INSTRUMENTOS DE RECOLECCIÓN DE DATOS

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

CUESTIONARIO PARA MEDIR LA VARIABLE: DELITO INFORMÁTICO

INSTRUCCIONES*:* Estimados usuarios, estamos realizando una investigación titulada "EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO - UCAYALI 2022" tu respuesta es de suma importancia por ello debe leer de manera detallada y luego marque con un aspa (X) uno de las cinco alternativas.

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

Dimensiones	Ítems	Escala de medición				
		Siempre	Casi siempre	A veces	Siempre	Casi siempre
Acceso a una base de datos	1. ¿Cree usted que las entidades bancarias son el medio por la cual se vulnera los datos de las personas y quedan expuestos a posibles fraudes?					
	2. ¿Considera que se debería desarrollar políticas de protección de información en las instituciones bancarias?					
	3. ¿En algún momento sintió que su información personal fue filtrada por las instituciones financieras y ser víctimas de estafadores?					
Uso ilegal de la información	4. ¿Usted fue víctima de suplantación en alguna ocasión y le generó pérdidas económicas?					
	5. ¿Usted consideró que hicieron mal uso de su información personal las instituciones bancarias?					
	6. ¿Se siente vulnerable ante los estafadores por estar bancarizada?					

Lugar y fecha: Pucallpa, 05 de septiembre de 2022.

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CUESTIONARIO PARA MEDIR LA VARIABLE OPERACIONES FINANCIERAS

INSTRUCCIONES*:* Estimados usuarios, estamos realizando una investigación titulada "EL DELITO INFORMÁTICO Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS EN LOS BANCOS DE LA PROVINCIA CORONEL PORTILLO - UCAYALI 2022" tu respuesta es de suma importancia por ello debe leer de manera detallada y luego marque con un aspa (X) uno de las cinco alternativas.

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

Dimensiones	Ítems	Escala de medición				
		Siempre	Casi siempre	A veces	Siempre	Casi siempre
Operaciones Phishing	1. ¿Llegó a ser víctima en algún momento de robo por medios electrónicos?					
	2. ¿Considera que el uso de aplicativos bancarios lo hace más propenso hacia las estafas?					
	3. ¿Considera que las instituciones bancarias deben desarrollar estrategias que cuiden sus operaciones en línea?					
Gestión de riesgos	4. ¿Las instituciones bancarias deben desarrollar estrategias que cuiden a sus clientes ante posibles estafas o robos?					
	5. ¿Considera que se debería monitorear las operaciones sospechosas por las instituciones bancarias?					
Otorgamiento de Créditos	6. ¿Cree usted que las instituciones bancarias deberían asegurar que el préstamo que desembolses este asegurado sin ningún costo adicional?					
	7. ¿Consideras que las tarjetas de crédito deben contar con un seguro sin costos adicionales?					
	8. ¿Cree que los bancos deberían hacerse responsables de los fraudes o robos en sus agencias y dar soluciones rápidas?					

Lugar y fecha: Pucallpa, 05 de septiembre de 2022.

ANEXO 4: EVIDENCIAS FOTOGRÁFICAS




SALIDA