

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y
CONTABLES
ESCUELA PROFESIONAL DE CONTABILIDAD



“TRANSACCIONES EN EL MERCADO ELECTRONICO Y EL FRAUDE CON TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA”.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE CONTADOR PÚBLICO

AUTORES:

YESABEL MILAGROS RODRIGUEZ RUÍZ
SEGUNDO LINO RUÍZ TORRES

ASESOR:

DR. RUSVELTH PAIMA PAREDES

PUCALLPA – PERÚ

2021



UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

COMISION DE GRADOS Y TITULOS

“Año del Fortalecimiento de la Soberanía Nacional”



ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE: CONTADOR PÚBLICO

Siendo las 10:00 Hrs del día Viernes 04 de Marzo del 2022, en los ambientes del Salón de Grados y Títulos de la Facultad de Ciencias Económicas, Administrativas y Contables, en cumplimiento con lo señalado en los Artículos 17º y 18º del Reglamento de General de Grado Académico de Bachiller, Título Profesional y Título de segunda Especialidad Profesional, se reunió el jurado integrado por los docentes: **Dr. Juan José Palomino Ochoa (Presidente)**, **CPC. Jorge Armando Palacios Valera (Miembro)** y **Mg. Olmedo Pizango Isuiza (Miembro)**.

Se realizó la Sustentación de la Tesis Titulada: “**TRANSACCIONES EN EL MERCADO ELECTRÓNICO Y EL FRAUDE CON LAS TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA**”, por el/la/los Bachilleres en Contabilidad: **Rodríguez Ruiz Yesabel Milagros, EN FORMA PRESENCIAL:**

Qué; según el Artículo 21º del Reglamento General de Grado Académico de Bachiller, Título Profesional y Título de Segunda Especialidad Profesional, que a la letra dice:

“La evaluación se hará de acuerdo a la siguiente escala de calificaciones:

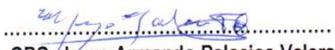
- Sobresaliente con felicitación escrita y recomendaciones de publicación
- Aprobado por unanimidad
- Aprobado por mayoría
- Desaprobado...”

El/la defensor(a) de la Tesis, ha obtenido la siguiente calificación;

Aprobado por unanimidad

Siendo las 11:00 Hrs del mismo día, se dio por concluido el acto y luego de ser leído el acta, los miembros del Jurado Evaluador procedieron a suscribirlo.


Dr. Juan José Palomino Ochoa
Presidente


CPC. Jorge Armando Palacios Valera
Miembro


Mg. Olmedo Pizango Isuiza
Miembro




Mg. Alex Davis Astohuaman Huaranga
Secretario Académico



UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE CIENCIAS ECONOMICAS, ADMINISTRATIVAS Y CONTABLES

COMISION DE GRADOS Y TITULOS

“Año del Fortalecimiento de la Soberanía Nacional”

**ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE:
CONTADOR PÚBLICO**

Siendo las *10:00 horas* del día Viernes 04 de Marzo del 2022, en los ambientes del Salón de Grados y Títulos de la Facultad de Ciencias Económicas, Administrativas y Contables, en cumplimiento con lo señalado en los Artículos 17º y 18º del Reglamento de General de Grado Académico de Bachiller, Título Profesional y Título de segunda Especialidad Profesional, se reunió el jurado integrado por los docentes: **Dr. Juan José Palomino Ochoa (Presidente), CPC. Jorge Armando Palacios Valera (Miembro) y Mg. Olmedo Pizango Isuiza (Miembro).**

Se realizó la Sustentación de la Tesis Titulada: **“TRANSACCIONES EN EL MERCADO ELECTRÓNICO Y EL FRAUDE CON LAS TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA”**, por el/la/los Bachilleres en Contabilidad: **Ruiz Torres Segundo Lino, EN FORMA PRESENCIAL:**

Qué; según el Artículo 21º del Reglamento General de Grado Académico de Bachiller, Título Profesional y Título de Segunda Especialidad Profesional, que a la letra dice:

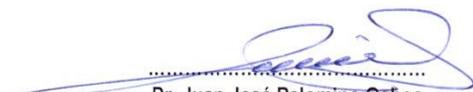
“La evaluación se hará de acuerdo a la siguiente escala de calificaciones:

- Sobresaliente con felicitación escrita y recomendaciones de publicación
- Aprobado por unanimidad
- Aprobado por mayoría
- Desaprobado...”

El/la defensor(a) de la Tesis, ha obtenido la siguiente calificación;

Aprobado por unanimidad

Siendo las *11:00 horas* del mismo día, se dio por concluido el acto y luego de ser leído el acta, los miembros del Jurado Evaluador procedieron a suscribirlo.


Dr. Juan José Palomino Ochoa
Presidente


CPC. Jorge Armando Palacios Valera
Miembro


Mg. Olmedo Pizango Isuiza
Miembro




Mg. Alex Davis Astohuaman Huaranga
Secretario Académico

ACTA DE APROBACIÓN

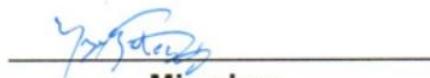
La presente tesis fue aprobada por el Jurado Calificador de la Facultad de Ciencias Económicas, Administrativas y Contables de la Universidad Nacional de Ucayali, para optar el Título Profesional de Contador Público.

Dr. Juan José Palomino Ochoa



Presidente

C.P.C Jorge Armando Palacios Valera



Miembro

Mg. Olmedo Pizango Isuiza



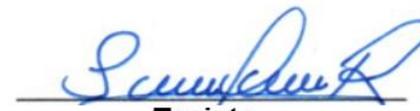
Miembro

Dr. Rusvelth Paima Paredes



Asesor

Yesabel Milagros Rodriguez Ruiz



Tesista

Segundo Lino Ruiz Torres



Tesista



UNIVERSIDAD NACIONAL DE UCAYALI
VICERRECTORADO DE INVESTIGACION
DIRECCION GENERAL DE PRODUCCION INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACION

SISTEMA ANTIPLAGIO URKUND

N°0302-2021

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

“TRANSACCIONES EN EL MERCADO ELECTRÓNICO Y EL FRAUDE CON TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA”

Cuyo(s) autor (es) : RODRIGUEZ RUÍZ, YESABEL MILAGROS
RUÍZ TORRES, SEGUNDO LINO

Facultad : CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES
Escuela Profesional : CONTABILIDAD
Asesor(a) : Dr. PAIMA PAREDES, RUSVELTH

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 6%**.

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 SELLA la presente constancia.

Fecha: 11/08/2021



Dr. ABRAHAM ERMITANIO HUAMAN ALMIRON
Dirección de Producción Intelectual



AUTORIZACIÓN DE PUBLICACION DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, YESABEL MILAGROS RODRIGUEZ RUIZ

Autor(a) de la TESIS de pregrado titulada:

"TRANSACCIONES EN EL MERCADO ELECTRÓNICO Y EL FRAUDE CON TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA"

Sustentada el año: 2022

Con la asesoría de: DR. RUSVELTH PAIMA PAREDES

En la Facultad: CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES

Escuela profesional: CONTABILIDAD

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 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 tiempo y 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 y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 28 / 04 / 2022

Email: yesabel1@hotmail.com
Teléfono: 926772673

Firma:
DNI: 72455278



AUTORIZACIÓN DE PUBLICACION DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, SEGUNDO LINO RUIZ TORRES

Autor(a) de la TESIS de pregrado titulada:

"TRANSACTIONS EN EL MERCADO ELECTRÓNICO Y EL FRAUDE CON TARJETAS DE CRÉDITO
Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA

Sustentada el año: 2022Con la asesoría de: DR. RUSVELTH PAIMA PAREDESEn la Facultad: CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLESEscuela profesional: CONTABILIDAD

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 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 tiempo y 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 y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 28 / 04 / 2022

Email: segundoruizt@hotmail.com
Teléfono: 977 216585

Firma:
DNI: 45874107

DEDICATORIA

A Dios por darme la vida y guiar siempre mi camino.

A mis padres por ser mi soporte e impulsarme a seguir adelante.

A nuestra querida Universidad Nacional de Ucayali.

A nuestros Docentes por ser parte de mi formación profesional.

Yesabel Milagros

A Dios por su amor infinito

A mis padres, que me han dado la existencia y en ello la capacidad para superarme y desearme lo mejor en cada paso por este camino difícil y arduo de la vida.

A mis hermanos, que con sus palabras de aliento no me dejaban caer para que siguiera adelante y perseverante y cumpla con mis metas.

Segundo Lino

AGRADECIMIENTO

A nuestra querida Universidad Nacional de Ucayali, con gratitud a la Escuela Profesional de Contabilidad.

A nuestros docentes que fueron parte de nuestra formación profesional.

A nuestro Asesor por sus aportes para lograr culminar nuestra investigación.

RESUMEN

La investigación presenta como objetivo general analizar la relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios de la ciudad de Pucallpa; los fraudes en los últimos años se ha incrementado significativamente que afectan a clientes de diferentes entidades bancarias y financieras, lo que genera incertidumbre y desconfianza en operaciones ante cajeros automáticos, por ello como objetivos específicos se ha analizado la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas, por otro lado se ha determinado la relación que existe entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero, que otro de los problemas que afectan a muchos clientes, por ello en la investigación se establece la relación existente entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa; la investigación es de tipo básica, de alcance relacional, diseño no experimental de enfoque cuantitativo, de acuerdo a los resultados obtenidos se concluye que existe relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios de la ciudad de Pucallpa.

Palabras clave: Mercado electrónico, Tarjetas de crédito y débito, Entorno virtual.

ABSTRACT

The general objective of the research is to analyze the relationship between transactions in the electronic market and fraud with credit and debit cards in the virtual business environment of the city of Pucallpa; Fraud in recent years has increased significantly, affecting customers of different banking and financial entities, which generates uncertainty and mistrust in ATM operations, for this reason, as specific objectives, the relationship between fraud due to data theft has been analyzed. in ATMs and the acceptance of the collaboration of private persons in the manipulation of jammed cards, on the other hand, the relationship between the telephone fraud of supposed bank employees and the obtaining of confidential data of the digital token key, ATM, which is another of the problems that affect many customers, so the investigation establishes the relationship between fraud by cloning cards for commercial operations and the lack of card key protection or not requesting the POS at the time of the transaction in the city of Pucallpa; The research is of a basic type, relational scope, non-experimental design with a quantitative approach, according to the results obtained it is concluded that there is a relationship between transactions in the electronic market and fraud with credit and debit cards in the virtual environment of business in the city of Pucallpa.

Keywords: Electronic market, Credit and debit cards, Virtual environment.

INTRODUCCIÓN

La investigación tiene como finalidad establecer el grado de relación existente entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios de la ciudad de Pucallpa, el repunte vertiginoso del comercio electrónico se ha sido maximizado con el COVID-19, en todo los campos del quehacer empresarial y de la sociedad en conjunto, por ello el comercio electrónico pasa por su máximo auge, el comercio en línea es totalmente natural en un mercado mundial en el que existen tiendas virtuales que masivamente ofrecen sus productos mediante redes, páginas y otros mecanismos electrónicos, en esa medida los riesgos financieros de las empresas y consumidores se incrementaron por la existencia de los fraudes electrónicos. A pesar que otro sector utiliza para sus operaciones el cajero automático en el que se generan riesgos por clonación o robo de claves, que afectan a los clientes de los bancos y entidades financieras.

La estructura de la investigación se ajusta al Reglamento de Grados y títulos que esta constituida de la manera siguiente:

En el capítulo I, se describe la problemática de acuerdo con el enfoque cuantitativo, se plantean los problemas, objetivos, hipótesis, justificación e importancia de la investigación, viabilidad y limitaciones de la investigación.

En el capítulo II, llamada estadio del arte, se presentan las investigaciones relacionadas al tema de investigación, teniendo en cuenta el ámbito internacional y nacional, asimismo, se presentan las bases teóricas, y las definiciones conceptuales de la investigación.

En el capítulo III, se sostiene la metodología empleada, para el presente es de tipo básica, con alcance relacional, diseño no experimental de enfoque cuantitativo, población y muestra, instrumento de recolección de datos y técnicas de recojo, procesamiento y presentación de datos.

En el capítulo IV, se exponen los resultados del trabajo de campo mediante tablas y figuras.

Capítulo V, se presentan las discusiones de resultados

Conclusiones

Sugerencia

Anexos

ÍNDICE

DEDICATORIA.....	viii
AGRADECIMIENTO.....	ix
RESUMEN.....	x
ABSTRACT.....	xi
INTRODUCCIÓN.....	xii
ÍNDICE.....	xiv
ÍNDICE DE TABLA.....	xv
ÍNDICE DE FIGURAS.....	xvi
CAPÍTULO I.....	12
CAPÍTULO II.....	19
CAPÍTULO III.....	43
CAPÍTULO IV.....	50
CAPÍTULO V.....	86
CONCLUSIONES.....	88
SUGERENCIAS.....	89
REFERENCIAS BIBLIOGRÁFICAS.....	90
ANEXOS	94

ÍNDICE DE TABLA

Tabla 1	Robo de datos en cajeros automáticos I_____	49
Tabla 2	Robo de datos en cajeros automáticos II_____	51
Tabla 3	Robo de datos en cajeros automáticos III_____	53
Tabla 4	Fraudes telefónicos – I_____	55
Tabla 5	Fraudes telefónicos – II_____	57
Tabla 6	Fraudes telefónicos – III_____	59
Tabla 7	Fraude clonación de tarjetas – I_____	61
Tabla 8	Fraude clonación de tarjetas – II_____	63
Tabla 9	Fraude clonación de tarjetas – III_____	65
Tabla 10	Manipulación de tarjetas atascadas en Cajeros Automáticos-I_	67
Tabla 11	Manipulación de tarjetas atascadas en Cajeros Automáticos-II_	69
Tabla 12	Manipulación de tarjetas atascadas en Cajeros Automáticos-III	71
Tabla 13	Obtención de datos confidenciales clave toquen digital – I____	73
Tabla 14	Obtención de datos confidenciales clave toquen digital – II____	75
Tabla 15	Obtención de datos confidenciales clave toquen digital – III____	77
Tabla 16	Protección de clave de tarjeta y POS – I_____	79
Tabla 17	Protección de clave de tarjeta y POS – II_____	81
Tabla 18	Protección de clave de tarjeta y POS – III_____	83

ÍNDICE DE FIGURAS

Figura 1	Robo de datos en cajeros automáticos I_____	50
Figura 2	Robo de datos en cajeros automáticos II_____	52
Figura 3	Robo de datos en cajeros automáticos III_____	54
Figura 4	Fraudes telefónicos – I_____	56
Figura 5	Fraudes telefónicos – II_____	58
Figura 6	Fraudes telefónicos – III_____	60
Figura 7	Fraude clonación de tarjetas – I_____	62
Figura 8	Fraude clonación de tarjetas – II_____	64
Figura 9	Fraude clonación de tarjetas – III_____	66
Figura 10	Manipulación de tarjetas atascadas en Cajeros Automáticos-I_	68
Figura 11	Manipulación de tarjetas atascadas en Cajeros Automáticos-II_	70
Figura 12	Manipulación de tarjetas atascadas en Cajeros Automáticos-III	72
Figura 13	Obtención de datos confidenciales clave toquen digital – I____	74
Figura 14	Obtención de datos confidenciales clave toquen digital – II____	76
Figura 15	Obtención de datos confidenciales clave toquen digital – III____	78
Figura 16	Protección de clave de tarjeta y POS – I_____	80
Figura 17	Protección de clave de tarjeta y POS – II_____	82
Figura 18	Protección de clave de tarjeta y POS – III_____	84

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

El avance vertiginoso de la era electrónica en el mundo ha sido maximizado con el COVID-19, en el que el uso se ha extendido para todo los efectos de la humanidad, incidiendo en la gestión empresarial, el comercio electrónico pasa por su máximo auge, el comercio en línea es totalmente natural en un mercado mundial en el que existen tiendas virtuales que masivamente ofrecen sus bienes de activos, productos mediante redes, páginas y otros mecanismos electrónicos, en esa medida los riesgos financieros de las empresas y consumidores se incrementaron por la existencia de los fraudes electrónicos.

Las empresas en los ultimos años utilizan medios electrónicos diversos en las adquisiciones de bienes y servicios y con mayor frecuencia el uso de las tarjetas de crédito y débito, por su versatilidad, siendo una tarjeta de débito un instrumento extendido a los clientes por los bancos y entidades financieras, que son empleados para operar por cajeros automáticos, o mediante dispositivos electrónicos mediante las APP de las entidades financieras mediante claves de SMS o toquen digital en el que se consultan en línea los saldos, depósitos, extracciones, pago de servicios, transferencias entre cuentas y, en general, la mayoría de las operaciones que pueden cursarse en línea o físicamente en los cajeros (AUDITOL, 2020).

El problema en nuestro país es que las tarjetas de débito y crédito no se diferencian ya que permiten realizar las mismas operaciones, sin embargo las

tarjetas de débito son los ahorros o fondos del propietario que tienen efecto directo, en cambio las tarjetas de crédito tienen otras características en sus transacciones como la de generar deudas a los usuarios y obligaciones que deben ser asumidos en el futuro, en ese sentido estos instrumentos son tan efectivas y en los últimos tiempos han agilizado las operaciones, en el que los usuarios no tienen que ir personalmente a las entidades bancarias o financieras para realizar operaciones, sin embargo existen modalidades de riesgos de fraude como las llamadas por teléfono, clonación de tarjetas y robo de datos en cajeros automáticos.

Los negocios en la actualidad comparten las transacciones en línea, de ahí el riesgo del fraude de las tarjetas de créditos y débitos, son exponencialmente altas, donde es notorio los fraudes de clonación de tarjetas de débito o crédito, las mismas son utilizadas por los ciber delincuentes, quienes utilizan múltiples medios para obtener información de la identidad de las personas y luego efectuar el robo de identidad o utilizan hackers con la finalidad de conseguir la clave y transferir a otras cuentas o efectuar compras dando la apariencia del titular.

Los negocios en la actualidad no efectúan un control de quienes son sus directivos o su personal de confianza, no efectúan la identificación de tipos de conducta, tampoco ponen en alerta ante el accionar irregular en el quehacer empresarial, o que las sospechas de ostentación de capacidad económica de algunos trabajadores de confianza, que alcanzan indicios de que algo ocurre en el negocio o son indicios de una red criminal en asociación con otros

negocios que vienen efectuando desvíos de fondos de las cuentas o ventas no registradas.

El control especializado es fundamental en las transacciones financieras en línea mediante el uso de las tarjetas de débito y crédito, así también en el retiro a través de cajeros automáticos, considerando evidencias de las operaciones y determinar las sospechas existentes sobre la presunta comisión de delitos o irregularidades, y de confirmarse el experto en control debe efectuar un informe sustentado sobre cómo se materializaron las irregularidades, quienes cometieron y facilitaron, que fallas humanas de procedimientos operativos e informáticos y contractuales las posibilitaron, hacer conocer el impacto monetario estimado del perjuicio sufrido por la organización, periodos y lugares donde acontecieron los hechos, (AUDITOL, 2020).

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿Cuál es la relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa?

1.2.2. PROBLEMAS ESPECÍFICOS

a) ¿Cuál es la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa?

- b. ¿Cuál es la relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa?
- c) ¿Cuál es la relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa?

1.3. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

1.3.1. OBJETIVO GENERAL

Analizar la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

1.3.2. OBJETIVOS ESPECÍFICOS

- a) Analizar la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.
- b) Determinar la relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.
- c) Establecer la relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o

no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

1.4. HIPÓTESIS

1.4.1. HIPÓTESIS GENERAL

Existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa.

1.4.2. HIPÓTESIS ESPECÍFICAS

- a) Existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.
- b) Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.
- c) Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

1.5. VARIABLES DE LA INVESTIGACIÓN

1.5.1. Variable 1: Transacciones en el mercado electrónico

- Fraude robo de datos en Cajeros Automáticos
- Fraude telefónico por supuestos funcionarios bancarios

- Fraude por clonación de tarjetas

1.5.2. Variable 2: Fraude con tarjetas de débito y crédito

- Colaboración de particulares en tarjetas atascadas
- Obtención confidencial de datos claves toquen digital
- Falta de protección de clave de tarjetas y POS

1.5.3. Operacionalización de las variables

1.6. JUSTIFICACIÓN E IMPORTANCIA

La investigación sobre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa, está completamente justificada porque con el avance de los medios electrónicos de pago en las transacciones comerciales el fraude del personal del procesador se han incrementado en el que proveen información de datos de los clientes a la delincuencia organizada para la generación de tarjetas clonadas de clientes reales en el entorno virtual de los negocios, asimismo el fraude del comerciante que efectúan cargos en la cuenta de tarjeta habientes operaciones que nunca realizaron en todo caso no fueron completadas o que fue pactada en diferentes condiciones y finalmente el fraude de los empleados del comercio en la sustracción de efectivo de caja sustituyendo ventas cobradas en efectivo por transacciones falsas con tarjetas de crédito.

Desde el enfoque cuantitativo la metodología de la investigación es básica objetivo, ya que busca ampliar conocimientos científicos ya existentes, desde la perspectiva del alcance es relacional por que mide el grado de asociación

entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa, de corte trasversal no experimental.

1.7. VIABILIDAD

La investigación por el objetivo que persigue es completamente viable, porque se cuenta con los instrumentos validados para el recojo de información de la muestra representativa de la unidad de análisis, que permite el desarrollo de la tesis.

1.8. LIMITACIONES

El estudio de las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa, en cuanto a sus limitaciones presenta cumplir los protocolos sanitarios como consecuencia del COVID-19.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1. ANTECEDENTES INTERNACIONALES

(Vásquez Rivera, 2019) en su tesis “Implementación de E-Commerce en una empresa que se dedica a la compra-venta de muebles para baño ubicada en el oriente de la ciudad de México”, en el que concluye que:

En la actualidad, el internet forma parte de la vida de la mayor parte de la población, ya sea por fines de entretenimiento, educativos, de negocios o por necesidad, es tan grande su penetración que hoy en día ya podemos hacer casi todo por medio de la web y de esta forma evitamos largas filas, pérdida de tiempo, traslados, entre muchas otras cosas, lo cual se ha vuelto sumamente conveniente, ya que vivimos en la época de las prisas, todo el mundo siempre está corriendo, trasladarse por la ciudad es sumamente tardado, peor aún si hablamos de ello en días lluviosos, con plantones, marchas, mantenimiento vial y un sinnúmero de situaciones ya comunes, la mayoría de la población no tiene tiempo de ir al super, al banco, hacer compras en general, y el día que tiene tiempo decide no salir, también estamos en la época del sedentarismo, de preferir quedarnos en casa, de evitar el gentío, que provoca la quincena, un día festivo, un evento deportivo, cultural o de entretenimiento en general y a raíz de todo esto llegó el internet a

simplicarnos la vida, podemos pedir súper a domicilio y no sólo eso, también ropa, zapatos, muebles, comida, medicamentos y en cantidad de cosas, podemos evitar ir al banco, ya que podemos transferir o pagar todos los servicios vía banca electrónica, con tarjeta de crédito o débito, en tiendas de conveniencia y más.

(Hernández Mejía, 2018) en su tesis “El funcionamiento de comercio electrónico, categorías seguridad para usuarios y demografía de usos habituales, concluyen en:

La presente investigación surge por la necesidad de realizar un análisis del uso del comercio electrónico a través de internet y de las nuevas tecnologías que se utilizan hoy en día, y de cómo la población lo adopta como forma y estilo de vida. El documento está estructurado con la presentación breve de sus antecedentes del comercio electrónico e internet, se abordan aristas, tales como, ¿qué es el comercio electrónico?, ¿para qué sirve?, usos más habituales, formas seguras de compra, venta, de un bien o un servicio, las plataformas más utilizadas, medios de pago, seguridad, estudios de diagnóstico y comparativos y finalmente una amplia información para el uso del comercio electrónico. Se exploran distintas fuentes primarias y secundarias, cuya bibliografía se relaciona al final, y se han establecido a través de un lenguaje sencillo y de fácil comprender, la relación entre los elementos que son de interés en la investigación “El funcionamiento del comercio

electrónico, categorías y seguridad para usuarios” Finalmente se relacionan algunas conclusiones que sirven de interpretación sobre las tendencias de estas tecnologías y cómo éstos inciden en la productividad y competitividad de las empresas para poder hacer Negocio y de los Nuevos estilos de Vida Adoptados por la Sociedad en la Actualidad. La descripción de lo que encontraremos dentro de la presente investigación se muestra desglosada por capítulos.

(Muñoz Luque, Murcia Torres, & De los Rios Castro, 2019) en su tesis “Propuesta de un modelo de inteligencia de negocios para la selección y planificación de una plataforma digital presentada a las sociedades especializadas en depósitos y pagos electrónicos (SEDPE)”, concluyen:

El termino Fintech se encuentra compuesto por las palabras en inglés Finance y Technology, relacionando así la tecnología al servicio del mercado financiero. Las compañías que desarrollan este modelo de negocio se presentan en el mercado financiero como intermediario o en algún caso competidor para las entidades financieras sin serlo. Por tanto esta revolución en el sector financiero ha impactado principalmente en la percepción de como los clientes esperan recibir sus servicios, pagar sus responsabilidades, invertir y proteger su dinero; es por esto que a lo largo de este proyecto se presenta una propuesta de un modelo de inteligencia de negocios para seleccionar una herramienta digital, la cual permitirá acercar los servicios financieros como

realizar pagos y transacciones digitales para un Grupo financiero (Banco) interesado en sumarse en este ecosistema de innovación, experiencia, calidad y servicio.

(Rodríguez Bravo, 2020) en su tesis “Análisis de los delitos informáticos en base a la alteración y modificación mediante transferencia electrónica en modalidad tarjeta de crédito”, concluye:

De las preguntas 1 y 2 de la encuesta aplicada se puede concluir que el 60% de los expertos en Derecho consultados tiene entre cinco y ocho años de ejercicio profesional, lo que permite afirmar que la muestra cuenta con experiencia suficiente para dar credibilidad a sus respuestas. Se puede concluir además que el 80 % ha participado profesionalmente en el juzgamiento de delitos informáticos en la modalidad de fraude con tarjeta de crédito. 2. De las preguntas 3 y 4 se puede concluir que es relevante la experiencia existente en otros países siendo esto fundamental para enfrentar adecuadamente el delito informático en el Ecuador; de los encuestados el 70% consideró que ese estudio es necesario para la adecuada seguridad informática. 3. De las preguntas 5 y 6 se concluye que dentro de los delitos informáticos realizados a través de la modalidad de fraude con tarjeta de crédito los más frecuentes son fraude por robo de identidad, fraude con pruebas a la tarjeta, fraude amistoso que, fraude de adquisición de cuenta 4. De las preguntas 7 y 8 llegamos a concluir que a diferencia de la pregunta

cinco, que se les solicitó información sobre los tipos de fraude más comunes con tarjeta de crédito, en esta se les pidió su opinión sobre las modalidades más frecuentes. Un 50% fue para la modalidad del uso de llave no autorizada que abre cualquier archivo del ordenador, siguiendo introducción de datos falsos y el uso de puertas falsas, de bombas lógicas o cronológicas. También se concluye sobre las causas de los delitos informáticos en común acuerdo en que radican en errores o descuidos atribuibles al propio usuario, indicios que la perpetración del delito se debe a errores de los propios consumidores, descuido en el manejo de equipos electrónicos donde se guardan los datos y claves de acceso. 5. De las preguntas 9 y 10 concluimos que entre los medios más utilizados para ejecutar los delitos informáticos se encuentra en un 60% el correo electrónico a través de las cuales personas desprevenidas o con habilidades limitadas en el manejo.

2.1.2. ANTECEDENTES NACIONALES

(Aruquipa Machicado, 2019) en su tesis “Auditoria Forense sobre tarjetas clonadas caso: Banco unión” concluye que:

Actualmente en Bolivia existen normas informáticas. La norma madre es la Ley N° 164 de Telecomunicaciones, que regula el comercio electrónico, la firma digital, el gobierno electrónico, la comunicación de datos transfronterizos. El Código Penal tipifica la Manipulación Informática artículo 363 bis y la Alteración, acceso y

uso indebido de datos informáticos 363 ter. como delito. Otro delito que se tiene tipificado es el acoso cibernético. Esta es una nueva figura legal que ha sido incluida en el Código Niño, Niña Adolescente, aprobado el 2015 en la Asamblea Legislativa Plurinacional, dice. La pena para quienes incurran en este delito será de entre cuatro y ocho años de privación de libertad. Existen otros delitos informáticos que son las formas más frecuentes en la actualidad; es decir, formas delincuenciales cometidas utilizando medios informáticos, así como el robo de información, suplantación de identidad, difamación, injurias o calumnias por internet y pornografía. Las redes sociales son motivo de tanta discusión, su regulación tendrá que ver con el Derecho Informático, nueva rama en el ámbito legal. Si acaso se logra esa medida, deberá ser analizada con moral y ética, valores que hoy pocos tienen. Derecho informático es el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información.

(Abanto Alejo, 2020) en su tesis “La clonación de tarjetas de crédito y la responsabilidad civil de la entidad financiera Los Olivos año 2020”, concluye que:

El tema de fraudes, realizados por la clonación de las tarjetas de crédito y la responsabilidad civil de la entidad financiera, como es

de conocimiento al ser un acceso fluido desde los distintas plataformas tanto físicas o virtuales; genera una ventaja y le da beneficios al usuario que otorga la entidad bancaria y/o financiera; es así que su utilidad también puede generar desventajas a la vez, puesto los avances y el desarrollo de tecnología ha llevado que el uso que una tarjeta sea también un riesgo ante el uso fraudulento por parte de terceros personas inescrupulosas que acceden a la cuenta usando métodos no permitidos a fin de cometer dichos actos. Para realizar esta investigación se optó por el marco metodológico de aceptación aplicado a un estudio cualitativo, el diseño es no experimental, con alcance exploratorio. Asimismo se comprobó el grado de la responsabilidad civil, que asume la entidad financiera frente al tarjetahabiente, en los temas generados por el fraude, en la modalidad de clonación, normativa nacional como es el código civil y el reglamento de tarjetas lo señala, a la vez se evaluó los procedimientos que son utilizados en tema de seguridad de información, aplicado al rubro de tarjetas de crédito y débito, el deber de proponer e innovar medidas prevención en favor del tarjetahabiente, ligados con el tema objeto de esta investigación y que generaría un gran alcance.

(Montoya Guillén, 2018) en su tesis “Regulación expresa del delito informático de clonación de tarjetas-sede DIVINDAT, 2017”, que tiene por:

Finalidad determinar la importancia de la tipificación expresa del delito de clonación de tarjetas, para su adecuado tratamiento; toda vez que actualmente está regulado de manera genérica y ambigua dentro de los delitos informáticos; y es en virtud a tal objetivo que a lo largo de la presente investigación se podrá evidenciar un amplio desarrollo sobre el tema del delito de clonación de tarjetas. La presente investigación es de tipo cualitativa y se encuentra orientado a la comprensión de un fenómeno socio-jurídico, para lograr nuestros objetivos se entrevistó a cinco funcionarios públicos investigadores especialistas en delitos informáticos de la sede DIVINDAT, además se entrevistó a cinco abogados especializado en la materia penal basado en su experiencia laboral y opinión sobre la investigación realizada. Los cuales proporcionaron información legal, además de brindar su punto de vista al tratamiento que se viene realizando al delito de clonación de tarjetas. Los resultados obtenidos en las entrevistas fueron sustentados con nuestro análisis documental, así como, con los resultados obtenidos de las investigaciones (tesis y artículos); llegando a concluir que el delito de clonación de tarjetas no está claramente tipificado y definido en la actual ley de delitos informáticos N° 30096, motivo por el cual ley actual es insuficiente frente a las nuevas modalidades que se presentan, ya que si bien tenemos el art. 8 sobre fraude informático no cumple con la

protección adecuada. Asimismo, se concluye basado en las entrevistas de los especialistas, sumado al análisis documental, y como se detalla en la discusión; surge la necesidad de establecer un tipo penal propio para garantizar la protección legal respecto al delito de clonación de tarjetas, además de poder perseguir el delito de forma directa teniendo ejemplos la legislación comparada; los países que regulan de manera específica son México, España y Venezuela que contrastan con la regulación aplicada en el Perú.

(García Donayre & Enero Santos, 2018) en su tesis "Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú", concluyen que:

La presente tesis denominada "Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú" surgió por la necesidad de lograr mitigar el gran número de fraudes que se vienen cometiendo contra los clientes de las entidades financieras del país, como contra las propias organizaciones financieras. Por tal motivo se desarrolló este proyecto, el cual brinda una herramienta informática a las organizaciones financieras, específicamente a la red de tiendas, agencias u oficinas de estas entidades, de este modo poder controlar los fraudes en la ejecución de los procedimientos bancarios, así como también permite gestionar y dar seguimiento mediante la generación de log en las transacciones que serán

derivados al área de riesgos. Para realizar este control y prevención de fraude, se desarrollaron mecanismos informáticos por medio de los cuales se realizará el bloqueo de operaciones para los colaboradores (cajeros) en las transacciones, en las que implique el uso de sus propias cuentas o su documento de identidad. La arquitectura de esta solución informática, se basa en SOA (Arquitectura Orientada a Servicios) para lograr integrar la información de entidades como RENIEC, SUNAT. Para el desarrollo del proyecto se utilizó el marco de desarrollo ágil “SCRUM”, se consultará la base de datos de los colaboradores y la base de datos de las cuentas, relacionándolas por el código de documento de identidad para que impida al colaborador (cajero) realizar operaciones en su propio terminal con sus cuentas. La plataforma del sistema será en entorno web para que pueda ser utilizado por todas las redes de tiendas de los diferentes distritos y provincias.

(Aures García & Boza Velez, 2018) en su tesis “Implantación de tecnología EMV en la Red ATM Banbif”, concluyen que:

El presente trabajo trata sobre la implantación de la seguridad de tarjetas de débito chip en la red de ATM del banco Banbif, este proyecto realizado en el año 2015 requirió del conocimiento de las reglas que rigen este entorno en cuanto a las marcas de estas tarjetas y los entes rectores de esta actividad, así como del dominio

de la metodología para la gestión de proyecto aplicada en la institución. Este trabajo consiste en la implantación de una de las más importante de estas reglas, el uso en los canales de la institución de tarjetas inteligentes o tarjetas chip para poder realizar transacciones en ellos, ahora, esta no impacta solamente en nuestro país sino se trata de esfuerzo mundial por erradicar el fraude realizado con las tarjetas clonadas sustrayendo información de sus legítimos poseedores.

(Del Pino Duran, Nieves Peñala, & Masias Pancorbo, 2019) en su tesis “La asimetría de la información y su incidencia en el nivel de endeudamiento de los usuarios de tarjetas de crédito del Banco Internacional del Perú – Tienda Real Plaza Cusco año 2018”, concluyen que:

El presente trabajo tiene como principal objetivo identificar la relación que existe entre la asimetría de información y la incidencia sobre el nivel de endeudamiento de los usuarios de tarjetas de crédito de la tienda Real Plaza Cusco del banco Internacional del Perú Interbank año 2018, para lo cual aplicaremos un modelo no experimental, a través de encuestas mostraremos la dependencia a corto y largo plazo de nuestras variables que son el nivel de endeudamiento y la asimetría de información. Se trabajó con un modelo no experimental descriptivo a través de encuestas donde la población fue de 11, 225 personas y la muestra de 194 personas,

para lo cual se validó la data mediante el coeficiente Alfa de Cronbach y se determinó mediante la prueba no paramétrica Tau-B-Kendall que los datos no cumplen una distribución normal, es decir tienen una relación inversa, a menor información brindada por el banco existe mayor nivel de endeudamiento, por tanto concluimos que la asimetría de información incide negativamente en el nivel de endeudamiento de los usuarios de tarjetas de banco Interbank agencia Cusco Real Plaza.

(Suarez Beltrán & Perea Obregón, 2018) en su tesis “Auditoria forense como herramienta en la detección del fraude financiero”, concluyen que:

Surge de la necesidad interna de explorar y obtener distintos conocimientos, ampliando el panorama ya expuesto referente a la auditoria, en Colombia se han visto avances significativos judicializando pruebas otorgadas mediante la auditoria forense, ya que esta provee las evidencias necesarias para enfrentar los delitos cometidos por funcionarios y empleados del cualquier sector económico, y ofrece un medio formal para poder controlar los múltiples fraudes cometidos en perjuicio de las empresas o instituciones, si bien es cierto la auditoria forense está siendo aplicada en el país, también es cierto que no es del conocimiento de muchos, generando falencias en el sector empresarial siendo expuesto a la práctica de fraudes y en el sector educativo, limitando la oportunidad de los egresados de Contaduría Pública u otras

profesiones afines de aspirar a su desarrollo un nuevo campo laboral. Esta investigación comprende un desarrollo progresivo de diferentes etapas que inicia desde la recopilación bibliográfica hasta la solución del porque la auditoria forense es una herramienta útil para detectar los fraudes financieros, debido a que esta proporciona un conocimiento amplio sobre fraudes, permitiendo explorar el campo de acción del defraudador para así realizar una detección precisa mediante la aplicación de sus fases. De esta manera se puede concluir que con la implementación de la auditoria forense como una herramienta de ayuda para prevenir y detectar los fraudes las empresas fortalecen el sistema de control interno y de esta forma protegen su patrimonio.

2.2. BASES TEÓRICAS

2.2.1. TRANSACCIONES EN MERCADOS ELECTRONICOS

Según (Martinez Hernández, 2014) sostiene que:

El mercado financiero internacional se desarrolla en estrecha simbiosis con las redes y las tecnologías intelectuales de soporte digital y tienden hacia una especie de inteligencia colectiva. Es de gran importancia la construcción de colectivos inteligentes, pues son estos los que determinarán el futuro de la economía (y de la cultura en general); ya no será la obtención de dinero virtual sino la capacidad creativa de construir conocimiento lo que determine la riqueza de un pueblo, grupo o individuo. En la actualidad, la información y el conocimiento son bienes

económicos, fuentes de producción y de riqueza. El conocimiento ha dejado de ser estable, las posibilidades son infinitas, por tal razón hay que adentrarse en nuevas búsquedas que develen otros tipos de riquezas. Además, la relación con el conocimiento ha cambiado. Cada vez que se introduce una nueva tecnología o cambia la configuración socioeconómica se pone en cuestión la jerarquía y el orden de los conocimientos. Por esta razón el saber debe ser una figura móvil, convertirse en flujo. El conocimiento ya no está anclado en un soporte material lo que le permite viajar, desplazarse de un individuo a otro, de un individuo a un procesador o de un procesador a otro. La circulación de conocimiento ha ampliado su objeto; dejó de estar encerrado en ámbitos como la academia y los expertos para hacer del total de ciudadanos su objeto. (p.31).

2.2.1.1. MERCADO ELECTRONICO

(Gariboldi, 1999) señala que:

En la actualidad, el crecimiento del comercio electrónico es un hecho innegable e irreversible. No sólo es así, sino que, según se prevé, continuará creciendo en los próximos años generando grandes ingresos a través de la red y ejerciendo su impacto sobre las actividades económicas y sobre el marco social dentro del cual estas tienen lugar. Por consiguiente, tanto en lo comercial como en lo técnico y lo social; a nivel individual, empresarial y gubernamental, será necesario "tomar conciencia

de esta nueva realidad". De ahí la importancia de estar preparados para competir en el mercado y para poder capitalizar los diversos beneficios que el comercio electrónico ofrece. En el contexto de la tecnología digital, el comercio electrónico dejó de ser una oportunidad para convertirse en un requerimiento más a los fines de poder operar. Ya no es una opción sino una necesidad. Participar de él permitirá mantener (o mejorar) la competitividad general de personas, empresas, regiones y países. Mantenerse al margen será sinónimo de aislamiento y, probablemente, ostracismo económico y social. A pesar que esta forma de comercio representa tan sólo una mínima parte del comercio total - menos del 0,5% del total de operaciones comerciales en los países industrializados (OCDE [1999]) - se espera que en un futuro constituya una parte significativa. No debe olvidarse que ya existe toda una generación de personas - personas que actualmente tienen entre 1 y 21 años electrónicos forma parte habitual de sus vidas. Ellos han tenido que usar una PC durante su educación, observan el funcionamiento de Internet como algo normal y se adaptan con gran facilidad a los continuos cambios de la oferta tecnológica. Esta generación ha estado expuesta al fenómeno de la globalización y, por lo tanto, la posibilidad de interactuar con personas o empresas ubicadas en cualquier rincón del planeta se les presenta y la perciben

como un aspecto de su realidad cotidiana. Lo que antes era un fenómeno aislado y particular como los "amigos por correspondencia" lo viven como un hecho diario gracias a los foros de discusión, los chats habitaciones etc. (p.1).

2.2.1.2. EL COMERCIO Y LA FUNCION EN EL TIEMPO

El comercio tradicional solo funciona durante ciertos períodos de tiempo, es decir durante determinados horarios o durante ciertas épocas del año. En dicho comercio, las respuestas a los estímulos producidos por los actores pueden tomar días, semanas y hasta meses. Si una empresa determinada decide, por ejemplo, presentar un producto nuevo o lanzar un mensaje a sus clientes potenciales tardará su tiempo en conocer los resultados y requerirá aún más tiempo para modificarlos en caso de ser necesario. El comercio electrónico no involucra horarios. Trabaja 24 horas al día, los 365 días del año. Ópera permanentemente un agente electrónico que es capaz de brindar los datos requeridos, tomar pedidos u ofrecer variedad de servicios. De igual modo interactúa, obtiene información y la transforma en conocimiento en tiempo real, sin demoras y casi instantáneamente. Actores Como se ha visto en el punto anterior, los actores del comercio electrónico pueden no ser humanos. (Gariboldi, 1999).

2.2.2. FRAUDE TARJETAS DE DEBITO Y CREDITO

La generalización del uso de las tarjetas de crédito y débito ha provocado un fuerte incremento de delitos relacionados con ellas. Concretamente ha disparado los fraudes en su utilización. Estos fraudes se pueden cometer tanto en los pagos efectuados en comercios, en los realizados a través de redes telemáticas, así como en la extracción ilegítima de dinero en cajeros automáticos. También ha multiplicado las conductas de falsificación de estos medios de pago. El presente artículo se ocupa de analizar cuál es la respuesta que ofrece el Derecho Penal para combatir esta clase de comportamientos, (Javato Martín, 2013).

(Durango Rodriguez, Roldan, Rincon, & Taborda, 2017) los diversos problemas de fraude presentados a nivel nacional, como una realidad inherente en nuestra sociedad y que trae consigo consecuencias a las personas, la importancia de este trabajo es realizar una investigación acerca de este tipo de acontecimientos presentados en el ámbito bancario. Su objetivo principal es dar a conocer y analizar la problemática actual en materia de fraudes por clonación de tarjetas ya que en la actualidad es una problemática de interés nacional que afecta a gran cantidad de persona que utiliza los medios electrónicos. La investigación de esta problemática se realizó por el interés de los integrantes del grupo, en conocer las maneras de realizar fraude y la desinformación de las personas con respecto a este tema y así tener una proyección enfocada al proceso de seguridad llevado por los bancos

para minimizar este tipo de sucesos. En este trabajo se visualiza una realidad que se vive en nuestra ciudad y todo nuestro país con respecto a los fraudes realizados directamente como clonación de las tarjetas de entidades bancarias y afectan directamente la economía de los colombianos por las pérdidas de dinero como consecuencia de este hecho lamentable. La característica principal de este tipo hechos es que se puede realizar de la manera más simple sin que la persona lo note, en ocasiones por tener un exceso de confianza la cual tiene mucho que ver con nuestra cultura o por desconocimiento de este tipo de prácticas.

2.2.2.1. RESPONSABILIDAD EN LOS FRAUDES CON TARJETAS DE PAGO

(Castro Acosta, 2013) señala que:

Actualmente, el uso de las tarjetas bancarias en sus distintas modalidades es la forma más sencilla de gestionar el dinero de una cuenta bancaria, ya que permite pagar en casi cualquier negocio, por teléfono o también por internet, además de hacer posible obtener efectivo en cualquier lugar mediante el uso de cajeros automáticos. Pero también existe un importante riesgo de fraude, en el que surge la cuestión de quién deberá soportar los daños causados por un pago fraudulento, si el cliente, el banco o el establecimiento, por lo que estudiamos la evolución que ha tenido la legislación en el campo de los servicios de pago, las disposiciones legales que regulan la responsabilidad en los

pagos no autorizados y hacemos un estudio de la jurisprudencia existente en nuestro país sobre este tema.

2.2.2.2. FRAUDE DEL COMERCIO

(AUDITOL, 2020), El fraude más común del comerciante es cargar en la cuenta de tarjeta habientes operaciones que nunca se realizaron, o cuya contra prestación no fue completada, o que fue pactada en diferentes condiciones, como, típicamente, por un importe menor. Si bien esta era una modalidad más fácilmente ejecutable en un entorno de cupones de compra impresos en papel y se redujeron con la masificación de los POS, las transacciones por Internet han vuelto a presentar la oportunidad, para los comerciantes inescrupulosos, para ejecutar este tipo de fraudes. El POS, inversamente, facilitó la captura de información de tarjeta habientes por los comerciantes para proceder con la clonación de tarjetas, el otro fraude común de parte de los comerciantes. (p.6).

FRAUDE DE LOS EMPLEADOS DEL COMERCIO

(AUDITOL, 2020), un mecanismo del que pueden disponer los empleados infieles para sustraer efectivo de la caja es sustituir ventas cobradas en efectivo por transacciones falsas con tarjetas de crédito. De tal forma, el arqueo no registra novedades, pero luego las operaciones ficticias son reclamadas por las tarjetas habientes. En cuyo caso, el empleado infiel

cuenta aún con el recurso de argumentar ante su empleador que quien está accionando fraudulentamente es el cliente que desconoce la compra realizada.

La circunstancia desafortunada para los comerciantes es que, ante recurrentes casos de fraudes originados en un mismo comercio tanto los procesadores como los Bancos o Entidades Financieras optan por cancelar el vínculo comercial imputando la responsabilidad al propietario del comercio, sin entrar a analizar si este fue o no victimizado por alguno/s de su/s dependiente/s. (p.6-7)

2.2.2.3. FRAUDE DE LOS EMPLEADOS DEL COMERCIO

(AUDITOL, 2020), un mecanismo del que pueden disponer los empleados infieles para sustraer efectivo de la caja es sustituir ventas cobradas en efectivo por transacciones falsas con tarjetas de crédito. De tal forma, el arqueo no registra novedades, pero luego las operaciones ficticias son reclamadas por las tarjetas habientes. En cuyo caso, el empleado infiel cuenta aún con el recurso de argumentar ante su empleador que quien está accionando fraudulentamente es el cliente que desconoce la compra realizada.

La circunstancia desafortunada para los comerciantes es que, ante recurrentes casos de fraudes originados en un mismo comercio tanto los procesadores como los Bancos o Entidades

Financieras optan por cancelar el vínculo comercial imputando la responsabilidad al propietario del comercio, sin entrar a analizar si este fue o no victimizado por alguno/s de su/s dependiente/s.

2.2.2.4. FRAUDE DE TARJETA HABIENTE

El fraude más característico de la tarjeta habiente es el de intentar repudiar operaciones que efectivamente ha realizado, tanto extracciones en ATM como en comercios. En ocasiones por imposibilidad de pagarlas, y en otros casos porque tales consumos pueden generar desavenencias familiares:

- Compras por las personas con tarjeta adicional en oposición a lo indicado por el titular de la cuenta. En casos extremos, cónyuges que vacían la tarjeta después de una desavenencia con su pareja
- Situaciones conflictivas como consumos que indicarían una presumible infidelidad
- Adicciones, por ejemplo, individuos que realizan consumos en estado de ebriedad y luego no los recuerdan Otro fraude más controvertido es cuando el tarjetahabiente (usuario de una tarjeta de crédito o débito) extravía su tarjeta (o eso dice...) y la misma es usada con posterioridad, pero antes que el cliente denuncie la pérdida. (AUDITOL, 2020).

2.3. DEFINICIONES CONCEPTUALES

2.3.1. Auditoría de sistemas:

Según (UNIREMINGTON, 2016), son los procesos sistemáticos que se encarga de evaluar el cumplimiento de las normas, la aplicación técnica y el desarrollo de procedimientos que se hacen en una organización con el fin de determinar la confidencialidad, confiabilidad, la seguridad, oportunidad, de la información que se prepara, produce y almacena por medio de la utilización de los sistemas de información. Por tanto, la Auditoría de los sistemas de información pertenece a una de las líneas especializadas de la auditoría la cual abarca el examen y verificación de los aspectos relacionados con los sistemas de información; los cuales se examinan también los procedimientos no automáticos que tiene que ver con ellos y las interfaces que les corresponde. Los elementos que se deben de tener en cuenta en la auditoría de sistemas: Desarrollo de sistemas (controles y metodología aplicada); seguridad área de informática; Planes de contingencia (respaldos, cuando se presentan fallas); Recursos Informáticos (control, resguardo y cuidado de los activos); Control a las modificaciones de aplicaciones (fraudes) y programas, contratos con los proveedores, evaluación a la utilización de los sistemas operativos y programas ; base de datos (como se desarrollan las aplicaciones), verificación a la red de teleprocesos, desarrollo del software de auditoría. El fin de la auditoría de sistema es la opinión sobre la confiabilidad de los sistemas de información que se

forma el auditor externo e interno, así como también la eficacia de las operaciones que realiza la oficina de tecnología e informática o quienes hagan sus veces.

2.3.2. Auditoria Especial a los Sistemas de información:

Es la verificación, seguimiento y monitoreo a los planes de mejoramiento de auditorías anteriores a los sistemas de información y cuya valoración resultó deficiente. (UNIREMINGTON, 2016).

2.3.3. Fraude financiero:

(Superintendencia de Banca y Seguros, 2020), por lo general la población es más sensible a estos delitos son los adultos mayores ya que cuentan con la mayor disponibilidad de liquidez de pago inmediato. Verifique que la empresa en la cual realizará sus depósitos sea una entidad supervisada por la SBS.

2.3.4. Fraude

La palabra fraude viene del latín FRAUD, que consiste en una acción que resulta contraria a la verdad y a la rectitud, el fraude se comete en perjuicio de una persona u organización, también es considerado como la utilización de una conducta deshonesta o engañosa con el fin de obtener alguna injusta ventaja sobre otra persona u organización. La legislación penal colombiana, no contempla entre los tipos penales el “fraude” como una conducta delictiva, encontrándose solamente el FRAUDE MEDIANTE CHEQUE y el FRAUDE PROCESAL, como tipo penal específico, (Linares Galvan, 2020).

2.4. BASES EPISTÉMICOS

Las transacciones en el mercado electrónico y el fraude de tarjetas de crédito y débito, tiene como base epistémica en los señalado por (Millan, 1989), una actividad de evaluación que, de forma independiente dentro de una empresa, tienen por objeto la revisión de operaciones contables, financieras y de todo tipo, con el fin de prestar un servicio a la dirección. Es un control administrativo cuya función es la de medir y valorar la eficacia de otros controles.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. TIPOS DE INVESTIGACIÓN

La investigación es básica ya que se busca ampliar conocimientos sobre las transacciones en mercados electrónicos y el fraude en tarjetas de créditos y débitos en el entorno virtual, en el que se busca medir el grado de relación.

Sobre la investigación básica (Carrasco Diaz, 2007) señala:

“Es la que no tiene propósitos aplicativos inmediatos, pues solo busca ampliar y profundizar el caudal de conocimientos científicos existentes acerca de la realidad. Su objetivo de estudio lo constituye las teorías científicas, las mismas que las analiza para perfeccionar sus contenidos”.

(p.43).

Respecto al alcance de la investigación de acuerdo al objetivo es correlacional, considerando que las transacciones en mercados electrónicos y el fraude en tarjetas de créditos y débitos en el entorno virtual, guardan vinculación significativa. Respecto al alcance de la investigación correlacional (Palomino Ochoa J. J., Dominguez Cuellar, Palomino Ochoa, & Torres Soria, 2021) señalan que:

“Tiene como objetivo determinar el grado de calidad, categoría, valor que tienen relación y analogía entre variables, corresponde a este alcance la hipótesis correlacional”. (p.111).

3.2. DISEÑO Y ESQUEMA DE LA INVESTIGACIÓN

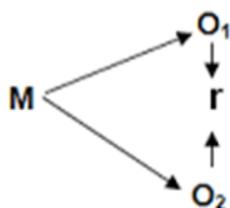
De acuerdo a la metodología planteada el diseño que mejor se adapta a la investigación de tipo básica es la no experimental.

(Carrasco Diaz, 2007) señala que:

“Son aquellos cuyas variables independientes carecen de manipulación intencional, y no poseen grado de control, ni mucho menos experimenta. Analizan y estudian los hechos y fenómenos de la realidad después de su ocurrencia”. (p.43).

Esquema

La investigación tendrá el siguiente esquema:



Donde:

M = Muestra

O1 = Observación Transacciones mercados electrónicos

O2 = Observación Fraude de tarjetas de débitos y créditos

r = relación entre variables

Margen de error:

Nivel de confianza:

Tamaño de Población:

Margen: 10%

Nivel de confianza: 99%

Población: 820

Tamaño de muestra: 138

$$n = \frac{z^2(p*q)}{e^2 + \frac{z^2(p*q)}{N}}$$

Ecuacion Estadistica para Proporciones poblacionales

n= Tamaño de la muestra

Z= Nivel de confianza deseado

p= Proporción de la población con la característica deseada (éxito)

q= Proporción de la población sin la característica deseada (fracaso)

e= Nivel de error dispuesto a cometer

N= Tamaño de la población

3.3. POBLACIÓN Y MUESTRA

3.3.1. POBLACIÓN

La población para el presente estudio es de 820 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa.

Respecto a la población o universo de una investigación dependerá del alcance de la investigación esta puede estar constituida por personas, procesos, cosas, animales, objetos, sucesos, etc. Sin embargo, el estudio puede estar constituida por una población significativa que requiere de una delimitación para su estudio, es ese contexto se obtendrá la muestra. (Palomino Ochoa J. J., Dominguez Cuellar, Palomino Ochoa, & Torres Soria, 2021).

3.3.2. MUESTRA

En ese contexto la muestra significativa está constituida de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa.

Con relación a la muestra esta debe ser representativa, tal como señalan (Palomino Ochoa J. J., Dominguez Cuellar, Palomino Ochoa, & Torres Soria, 2021), que:

“La muestra resulta de la delimitación efectuada del universo de estudio o también conocido como población, en el que por la magnitud requiere ser extraída del universo una parte que reúne las características de la población”.
(p.116).

3.4. OPERACIONALIZACIÓN DE LAS VARIABLES

VARIABLE	DIMENSIONES	INDICADORES
TRANSACCIONES EN EL MERCADO ELECTRÓNICO	Fraude robo de datos en Cajeros Automáticos	Proveer información de datos falsos de clientes a la delincuencia organizada
		Tarjetas clonadas
		Contraprestación no completada
	Fraude telefónico por supuestos funcionarios bancarios	Pactada en diferentes condiciones
		Importe menor
		Cupones de compra
	Fraude por clonación de tarjetas	Sustituir ventas cobradas
		Transacciones falsas
		Tarjetas de crédito
TARJETAS DE CRÉDITO Y DÉBITO	Colaboración de particulares en tarjetas atascadas	Arqueo
		Operaciones ficticias
		Acción fraudulenta
	Obtención confidencial de datos claves toquen digital	Compras por personas con tarjeta adicional
		Desavenencia con pareja
		Conyugues que vacían tarjetas
		Infidelidad
		Consumo en estado de ebriedad
Falta de protección de clave de tarjetas y POS		

3.5. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

(Carrasco Díaz, 2007), el método, en tanto se emplea para realizar investigaciones científicas, se denomina método científico y constituye un sistema de procedimientos, técnicas, instrumentos, acciones estratégicas y tácticas para resolver el problema de investigación, así como probar la hipótesis científica. Sin duda son numerosas las técnicas e instrumentos para la recolección de datos. (p. 269-282).

En ese contexto los instrumentos a utilizar en la presente investigación considerando el enfoque y el alcance son la encuesta mediante cuestionarios de las variables de estudio, a fin de establecer la relación entre ambas variables.

3.6. TÉCNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS

3.6.1. TÉCNICA DE RECOJO

La recolección de datos se realiza mediante la observación directa e indirecta del participante, no participante de una investigación cualitativa o cuantitativa, a través de la encuesta representada por cuestionario que están dadas por escalas de medición en cuanto a su confiabilidad, validez que pueden ser nominales, ordinales, intervalos iguales o cocientes o razones; la entrevista que puede ser estructurada o no estructurada. (Palomino Ochoa J. J., Dominguez Cuellar, Palomino Ochoa, & Torres Soria, 2021). (p.118).

3.6.2. LA ENCUESTA

La encuesta es una técnica para la investigación social por excelencia, debido a su utilidad, versatilidad, sencillez y objetividad de los datos que con ella se obtiene. Desde hace buen tiempo se le emplea con mucho éxito, en la investigación educacional, gracias a los resultados obtenidos con su aplicación.

Puntualmente la encuesta puede definirse como una técnica de investigación social para la indagación, exploración y recolección de datos, mediante preguntas formuladas directa e indirectamente a los sujetos que constituyen la unidad de análisis del estudio investigado, (Carrasco Díaz, 2007) (p.314).

EL CUESTIONARIO

Es el instrumento de investigación social más usado cuando se estudia gran número de personas, ya que permite una respuesta directa, mediante la hoja de preguntas que se le entrega a cada una de ellas. Las preguntas estandarizadas se preparan con anticipación y previsión, (Carrasco Díaz, 2007) (p.318).

3.6.3. PRESENTACIÓN DE DATOS

En la presentación de datos se emplearon el Excel que permite el proceso estadístico con el uso de del programa SPSS, en base a la estadística descriptiva, para presentar las tablas y figuras.

En cuanto a la tabulación de datos consiste en definir la forma de matrices de registro de información que se espera llenar a partir de los

datos obtenidos de las muestras representacionales. Para la codificación de la data e información obtenida, el software SPSS nos permite seleccionar la opción de presentar los resultados en cuadros tablas, gráficos, figuras, etc. (Arroyo Morales, Metodología de la investigación en las ciencias empresariales, 2020). (p.278).

CAPÍTULO IV

4. RESULTADOS

4.1. Dimensión: Robo de datos en Cajeros Automáticos

Existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.

Tabla 1.

Robo de datos en Cajeros Automáticos.

	f	h	H
Alta	103	74.64	74.64
Bajo	32	23.19	97.83
Ninguno	3	2.17	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

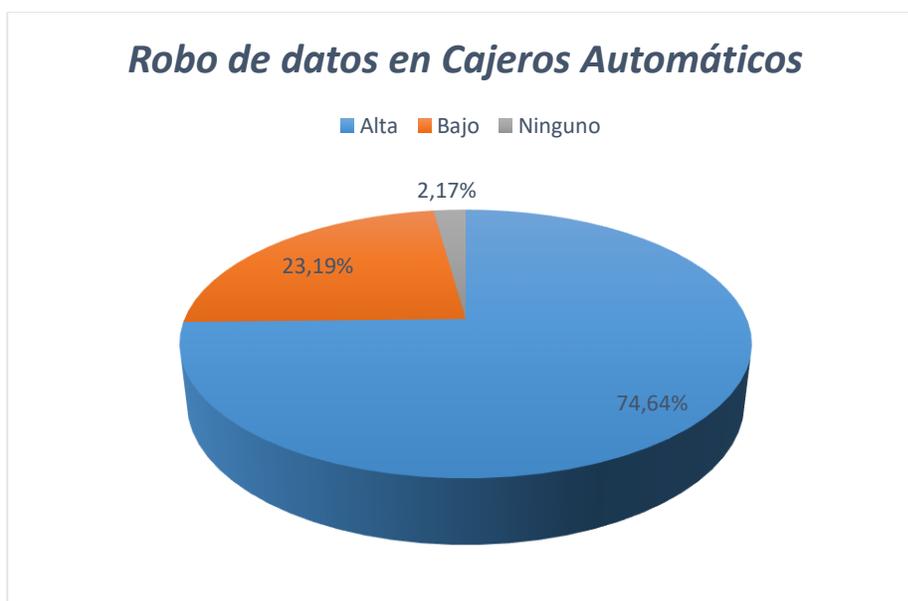
De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 103 personas que representa el 74.64% de los encuestados respondieron que existe un alto grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 32 personas que representa

el 23.19% de los encuestados respondieron que existe un bajo grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 3 personas que representa el 2.17% de los encuestados respondieron que no existe ningún grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.

Figura 1



4.2. Dimensión: Robo de datos en Cajeros Automáticos

Existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

Tabla 2.

Robo de datos en Cajeros Automáticos.

	f	h	H
Alta	94	68.12	68.12
Bajo	40	28.99	97.10
Ninguno	4	2.90	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

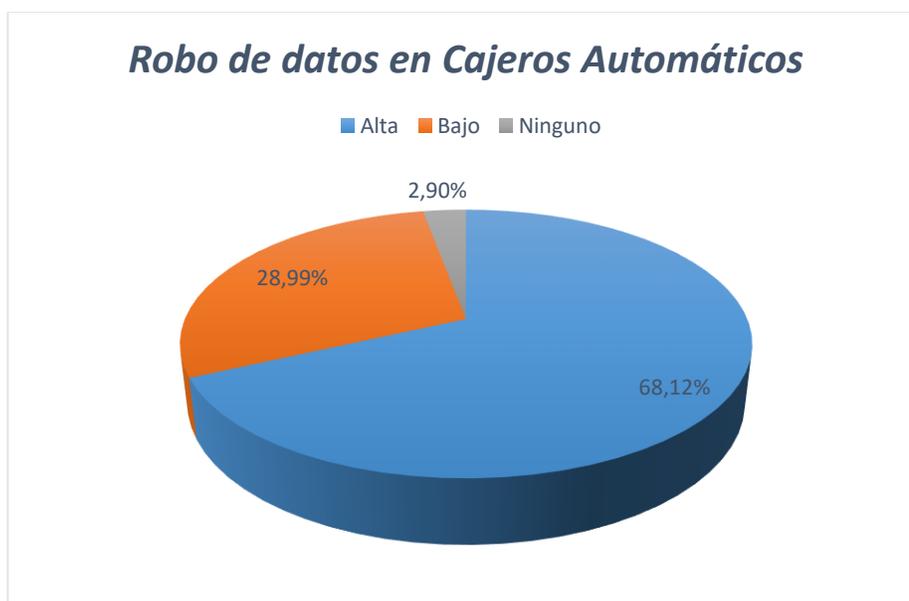
De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 94 personas que representa el 68.12% de los encuestados respondieron que existe un alto grado de relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 40 personas que representa el 28.99% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 4 personas que representa el 2.90% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

Figura 2



4.3. Dimensión: Robo de datos en Cajeros Automáticos

Existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

Tabla 3.

Robo de datos en Cajeros Automáticos.

	f	h	H
Alta	116	84.06	84.06
Bajo	15	10.87	94.93
Ninguno	7	5.07	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

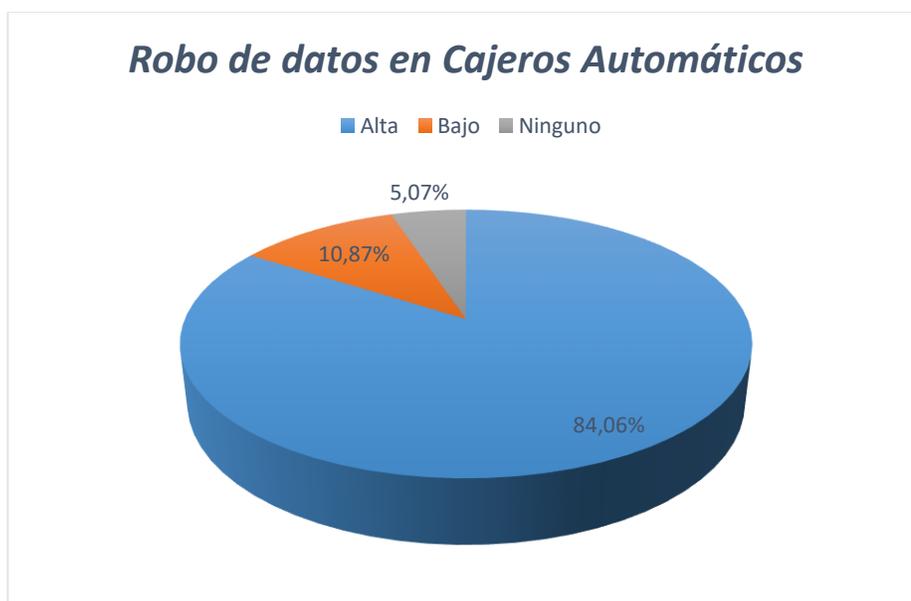
De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 116 personas que representa el 84.06% de los encuestados respondieron que existe un alto grado de relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 15 personas que representa el 10.87% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 7 personas que representa el 5.07% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

Figura 3



4.4. Dimensión: Fraudes telefónicos

Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

Tabla 4.

Fraudes telefónicos.

	f	h	H
Alta	109	78.99	78.99
Bajo	17	12.32	91.30
Ninguno	12	8.70	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

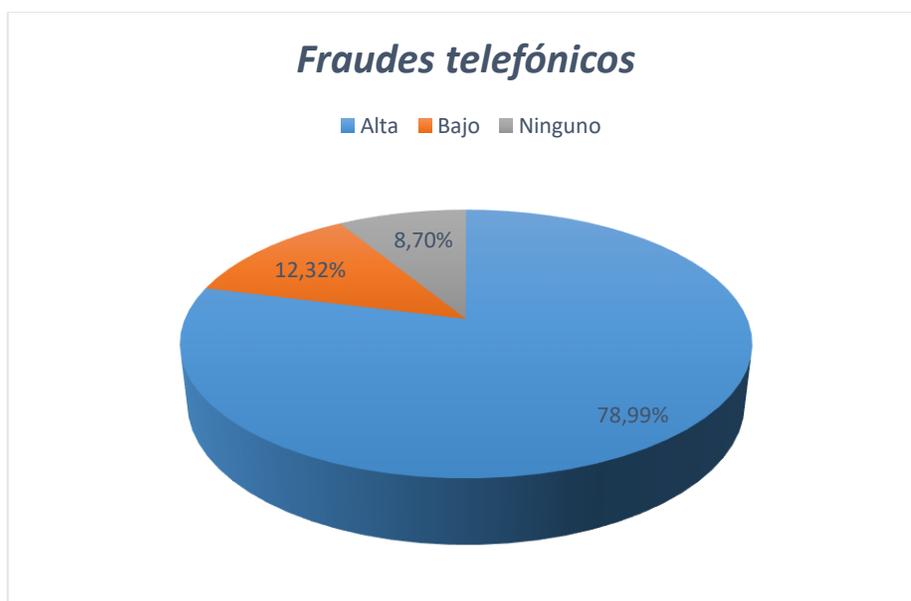
De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 109 personas que representa el 78.99% de los encuestados respondieron que existe un alto grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 17 personas que representa el 12.32% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 12 personas que representa el 8.70% de los encuestados respondieron que no existe ningún grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

Figura 4



4.5. Dimensión: Fraudes telefónicos

Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

Tabla 5.

Fraudes telefónicos.

	f	h	H
Alta	97	70.29	70.29
Bajo	25	18.12	88.41
Ninguno	16	11.59	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

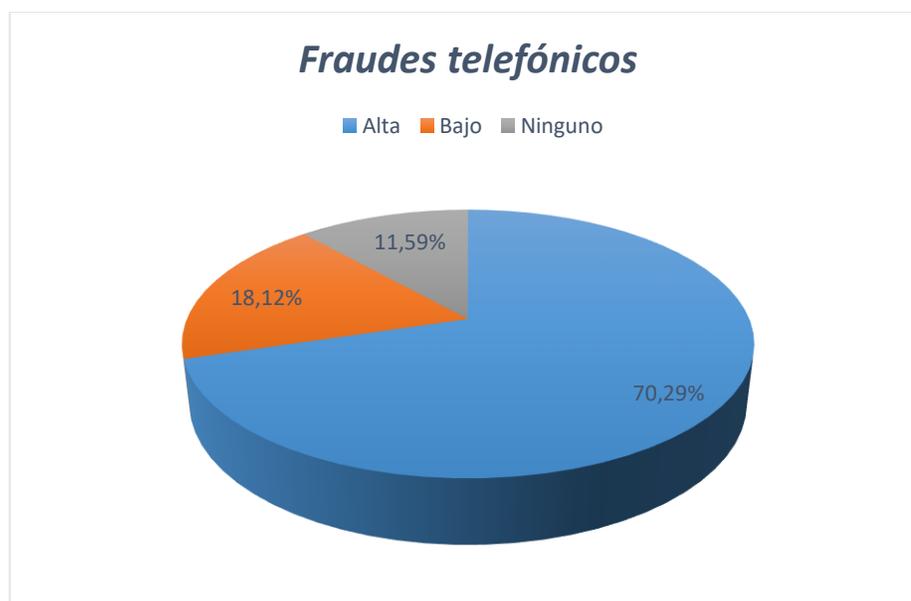
De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 97 personas que representa el 70.29% de los encuestados respondieron que existe un alto grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 25 personas que representa el 18.12% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 16 personas que representa el 11.59% de los encuestados respondieron que no existe ningún grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

Figura 5



4.6. Dimensión: Fraudes telefónicos

Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

Tabla 6.

Fraudes telefónicos.

	f	h	H
Alta	113	81.88	81.88
Bajo	24	17.39	99.28
Ninguno	1	0.72	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 113 personas que representa el 81.88% de los encuestados respondieron que existe un alto grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 24 personas que representa el 17.39% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 1 personas que representa el 0.72% de los encuestados respondieron que no existe ningún grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

Figura 6



4.7. Dimensión: Fraude clonación de tarjetas

Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

Tabla 7.

Fraude clonación de tarjetas.

	f	h	H
Alta	100	72.46	72.46
Bajo	28	20.29	92.75
Ninguno	10	7.25	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 100 personas que representa el 72.46% de los encuestados respondieron que existe un alto grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 28 personas que representa el 20.29% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 10 personas que representa el 7.25% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

Figura 7



4.8. Dimensión: Fraude clonación de tarjetas

Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

Tabla 8.

Fraude clonación de tarjetas.

	f	h	H
Alta	91	65.94	65.94
Bajo	36	26.09	92.03
Ninguno	11	7.97	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 91 personas que representa el 65.94% de los encuestados respondieron que existe un alto grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 36 personas que representa el 26.09% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 11 personas que representa el 7.97% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

Figura 8



4.9. Dimensión: Fraude clonación de tarjetas

Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

Tabla 9.

Fraude clonación de tarjetas.

	f	h	H
Alta	118	85.51	85.51
Bajo	18	13.04	98.55
Ninguno	2	1.45	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable Transacciones en el mercado electrónico

Fuente: Elaboración propia

Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 118 personas que representa el 85.51% de los encuestados respondieron que existe un alto grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 18 personas que representa el 13.04% de los encuestados respondieron que existe un bajo grado de

relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 2 personas que representa el 1.45% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

Figura 9



4.10. Dimensión: Manipulación de tarjetas atascadas en Cajeros Automáticos

Existe grado de relación entre el fraude por colaboración de particulares en la manipulación de tarjetas atascadas en los cajeros automáticos.

Tabla 10.

Manipulación de tarjetas atascadas en Cajeros Automáticos.

	f	h	H
Alta	101	73.19	73.19
Bajo	22	15.94	89.13
Ninguno	15	10.87	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

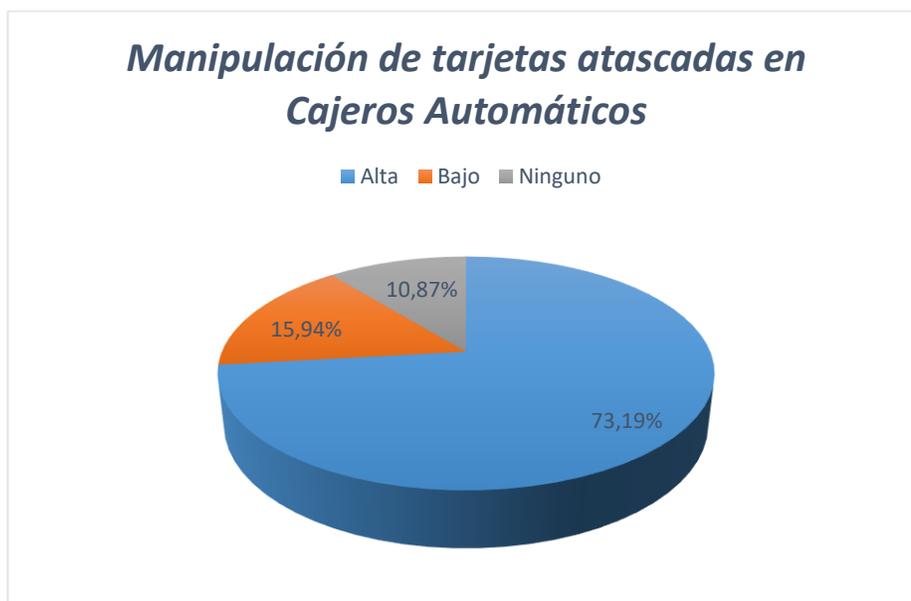
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 101 personas que representa el 73.19% de los encuestados respondieron que existe un alto grado de relación entre el fraude por colaboración de particulares en la manipulación de tarjetas atascadas en los cajeros automáticos.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 22 personas que representa el 15.94% de los encuestados respondieron que existe un bajo grado de relación entre el fraude por colaboración de particulares en la manipulación de tarjetas atascadas en los cajeros automáticos.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 15 personas que representa el 10.87% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por colaboración de particulares en la manipulación de tarjetas atascadas en los cajeros automáticos.

Figura 10



4.11. Dimensión: Manipulación de tarjetas atascadas en Cajeros Automáticos

Existe grado de relación entre el fraude por la falta de previsión de la exposición de clave por falta de descripción en la ciudad de Pucallpa.

Tabla 11.

Manipulación de tarjetas atascadas en Cajeros Automáticos.

	f	h	H
Alta	92	66.67	66.67
Bajo	33	23.91	90.58
Ninguno	13	9.42	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

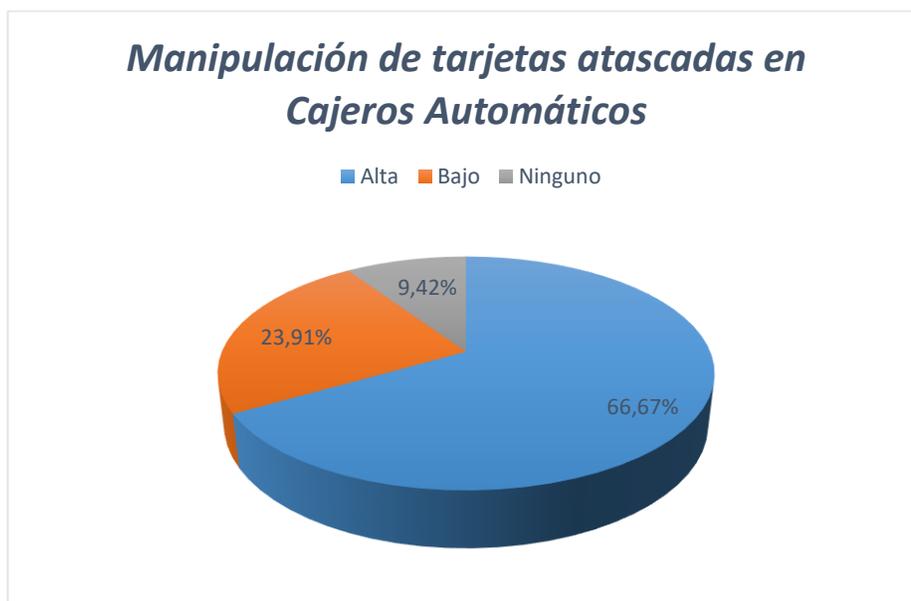
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 92 personas que representa el 66.67% de los encuestados respondieron que existe un alto grado de relación entre el fraude por la falta de previsión de la exposición de clave por falta de descripción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 33 personas que representa el 23.91% de los encuestados respondieron que existe un bajo grado de relación entre el fraude por la falta de previsión de la exposición de clave por falta de descripción en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 13 personas que representa el 9.42% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por la falta de previsión de la exposición de clave por falta de descripción en la ciudad de Pucallpa.

Figura 11



4.12. Dimensión: Manipulación de tarjetas atascadas en Cajeros Automáticos

Existe grado de relación entre el fraude por falta de previsión de objetos sobrepuestos en los cajeros automáticos de la ciudad de Pucallpa.

Tabla 12.

Manipulación de tarjetas atascadas en Cajeros Automáticos.

	f	h	H
Alta	106	76.81	76.81
Bajo	21	15.22	92.03
Ninguno	11	7.97	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

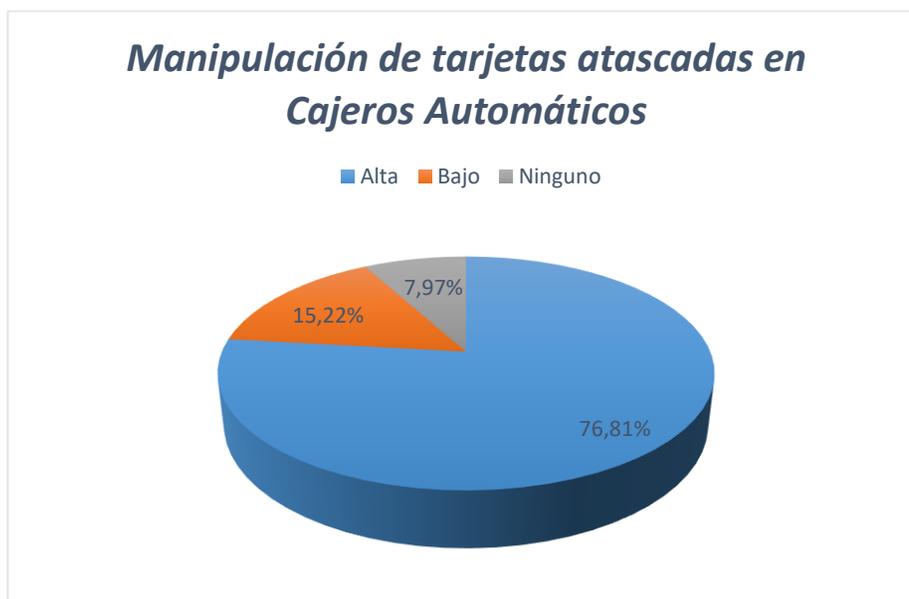
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 106 personas que representa el 76.81% de los encuestados respondieron que existe un alto grado de relación entre el fraude por falta de previsión de objetos sobrepuestos en los cajeros automáticos de la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 21 personas que representa el 15.22% de los encuestados respondieron que existe un bajo grado de relación entre el fraude por falta de previsión de objetos sobrepuestos en los cajeros automáticos de la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 11 personas que representa el 7.97% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por falta de previsión de objetos sobrepuestos en los cajeros automáticos de la ciudad de Pucallpa.

Figura 12



4.13. Dimensión: Obtención de datos confidenciales clave toquen digital

Existe relación entre el fraude por obtención de datos confidenciales de clave de toquen digital por simulación de llamadas de criminales.

Tabla 13.

Obtención de datos confidenciales clave toquen digital.

	f	h	H
Alta	111	80.43	80.43
Bajo	19	13.77	94.20
Ninguno	8	5.80	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

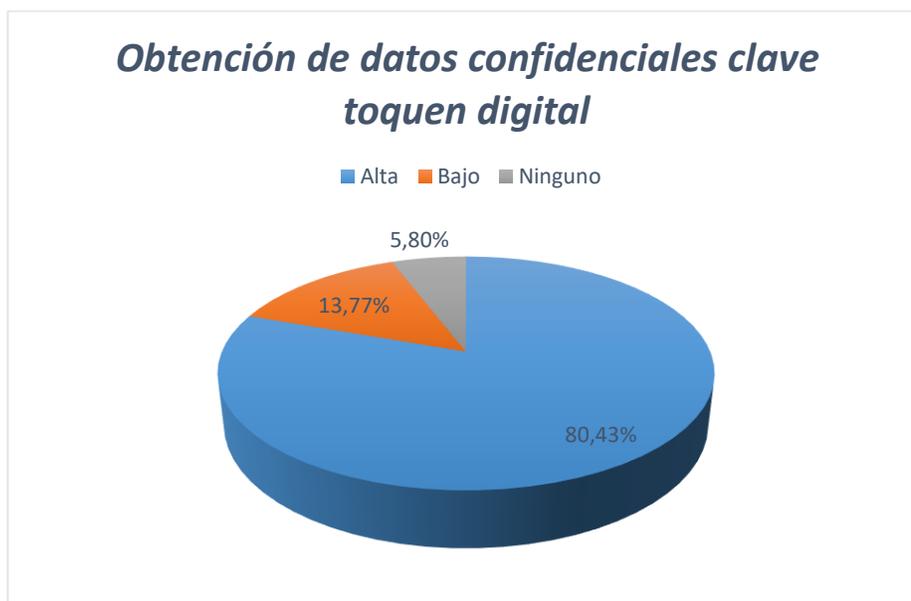
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 111 personas que representa el 80.43% de los encuestados respondieron que existe un alto grado de relación entre el fraude por obtención de datos confidenciales de clave de toquen digital por simulación de llamadas de criminales.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 19 personas que representa el 13.77% de los encuestados respondieron que existe un bajo grado de relación entre el fraude por obtención de datos confidenciales de clave de toquen digital por simulación de llamadas de criminales.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 8 personas que representa el 5.80% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por obtención de datos confidenciales de clave de toquen digital por simulación de llamadas de criminales.

Figura 13



4.14. Dimensión: Obtención de datos confidenciales clave toquen digital

Existe relación entre el fraude por obtención de datos confidenciales de clave de cajeros por simulación de llamadas de criminales.

Tabla 14.

Obtención de datos confidenciales clave toquen digital.

	f	h	H
Alta	95	68.84	68.84
Bajo	36	26.09	94.93
Ninguno	7	5.07	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

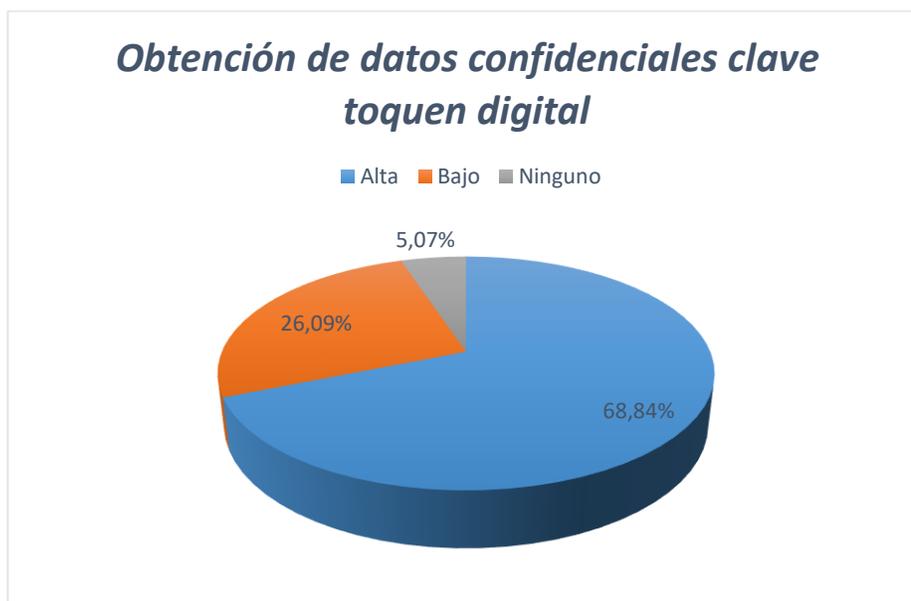
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 95 personas que representa el 68.84% de los encuestados respondieron que existe un alto grado de relación entre el fraude por obtención de datos confidenciales de clave de cajeros por simulación de llamadas de criminales.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 36 personas que representa el 26.09% de los encuestados respondieron que existe un bajo grado de relación entre el fraude por obtención de datos confidenciales de clave de cajeros por simulación de llamadas de criminales.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 7 personas que representa el 5.07% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por obtención de datos confidenciales de clave de cajeros por simulación de llamadas de criminales.

Figura 14



4.15. Dimensión: Obtención de datos confidenciales clave toquen digital

Existe relación entre el fraude por obtención de datos confidenciales de contraseña de la banca por simulación de llamadas de criminales tarjetas de habientes en la ciudad de Pucallpa.

Tabla 15.

Obtención de datos confidenciales clave toquen digital.

	f	h	H
Alta	114	82.61	82.61
Bajo	13	9.42	92.03
Ninguno	11	7.97	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

Análisis:

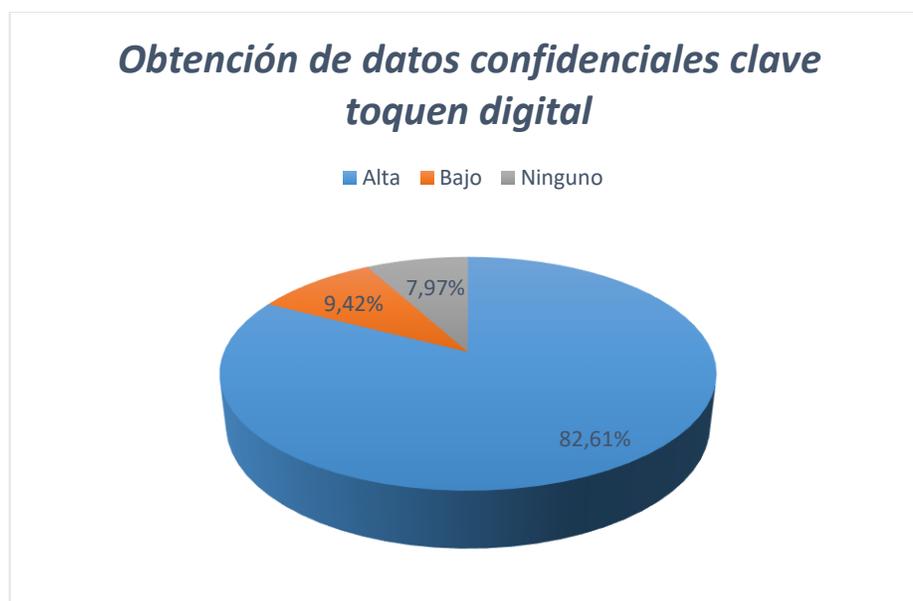
De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 114 personas que representa el 82.61% de los encuestados respondieron que existe un alto grado de relación entre el fraude por obtención de datos confidenciales de contraseña de la banca por simulación de llamadas de criminales tarjetas de habientes en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 13 personas que representa el 9.42% de los encuestados respondieron que existe un bajo grado de relación

entre el fraude por obtención de datos confidenciales de contraseña de la banca por simulación de llamadas de criminales tarjetas de habientes en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 11 personas que representa el 7.97% de los encuestados respondieron que no existe ningún grado de relación entre el fraude por obtención de datos confidenciales de contraseña de la banca por simulación de llamadas de criminales tarjetas de habientes en la ciudad de Pucallpa.

Figura 15



4.16. Dimensión: Protección de clave de tarjeta y POS

Existe grado de relación del fraude por falta de protección de clave de tarjetas en la ciudad de Pucallpa.

Tabla 16.

Protección de clave de tarjeta y POS.

	f	h	H
Alta	90	65.22	65.22
Bajo	45	32.61	97.83
Ninguno	3	2.17	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

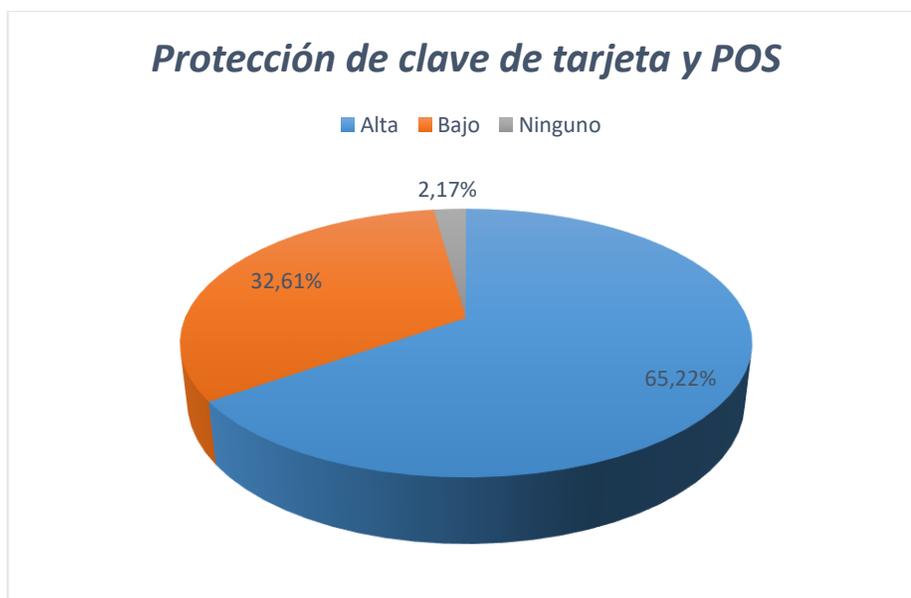
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 90 personas que representa el 65.22% de los encuestados respondieron que existe un alto grado de relación del fraude por falta de protección de clave de tarjetas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 45 personas que representa el 32.61% de los encuestados respondieron que existe un bajo grado de relación del fraude por falta de protección de clave de tarjetas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 3 personas que representa el 2.17% de los encuestados respondieron que no existe ningún grado de relación del fraude por falta de protección de clave de tarjetas en la ciudad de Pucallpa.

Figura 16



4.17. Dimensión: Protección de clave de tarjeta y POS

Existe grado de relación del fraude por falta de solicitud en el acto de POS por operaciones con tarjeta en la ciudad de Pucallpa.

Tabla 17.

Protección de clave de tarjeta y POS.

	f	h	H
Alta	98	71.01	71.01
Bajo	27	19.57	90.58
Ninguno	13	9.42	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

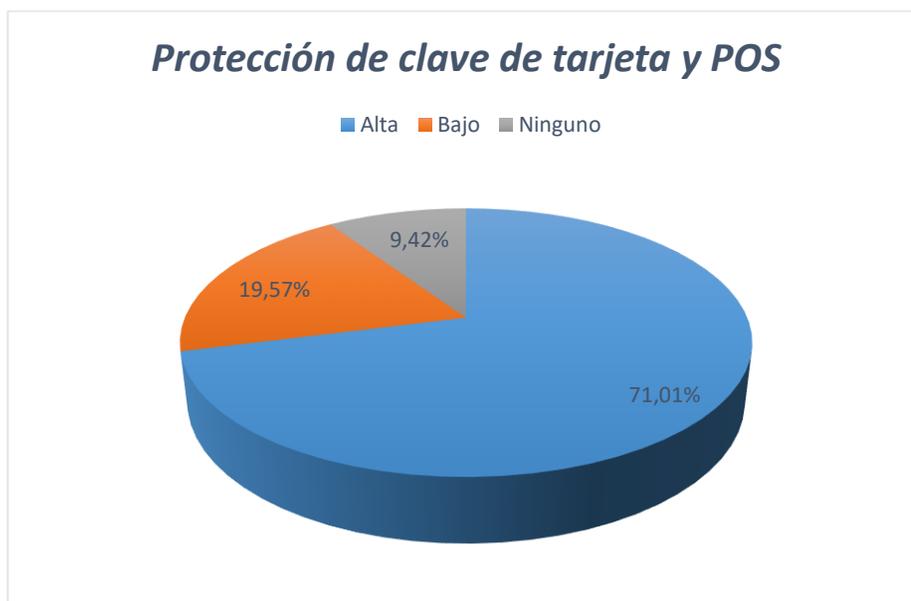
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 98 personas que representa el 71.01% de los encuestados respondieron que existe un alto grado de relación del fraude por falta de solicitud en el acto de POS por operaciones con tarjeta en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 27 personas que representa el 19.57% de los encuestados respondieron que existe un bajo grado de relación del fraude por falta de solicitud en el acto de POS por operaciones con tarjeta en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 13 personas que representa el 9.42% de los encuestados respondieron que no existe ningún grado de relación del fraude por falta de solicitud en el acto de POS por operaciones con tarjeta en la ciudad de Pucallpa.

Figura 17



4.18. Dimensión: Protección de clave de tarjeta y POS

Existe grado de relación del fraude por falta de protección de la contraseña de las tarjetas en operaciones realizadas en la ciudad de Pucallpa.

Tabla 18.

Protección de clave de tarjeta y POS.

	f	h	H
Alta	104	75.36	74.64
Bajo	19	13.77	89.13
Ninguno	15	10.87	100.00
Total	138	100 %	

Nota: Dimensión correspondiente a la variable fraude con tarjetas de crédito y débito.

Fuente: Elaboración propia

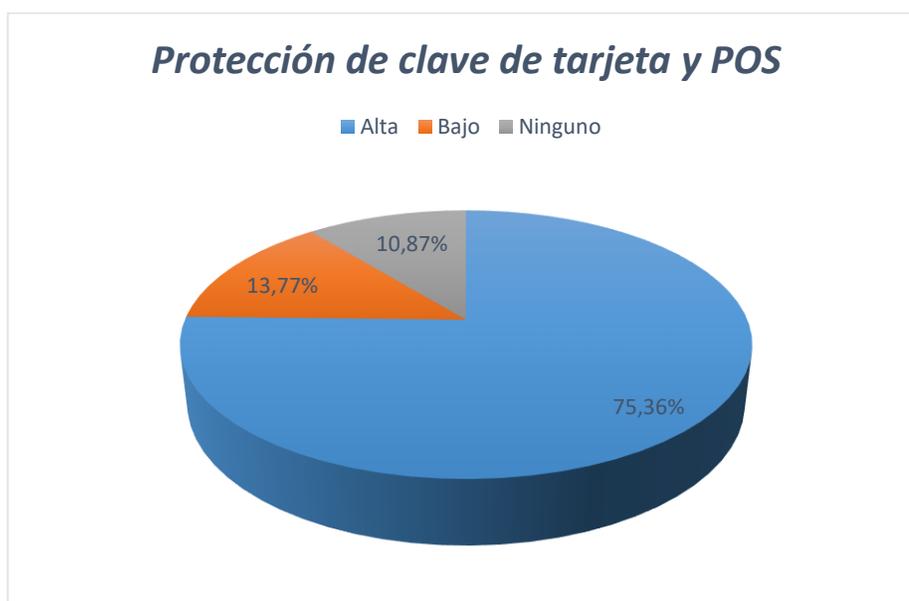
Análisis:

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 101 personas que representa el 75.36% de los encuestados respondieron que existe un alto grado de relación del fraude por falta de protección de la contraseña de las tarjetas en operaciones realizadas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 19 personas que representa el 13.77% de los encuestados respondieron que existe un bajo grado de relación del fraude por falta de protección de la contraseña de las tarjetas en operaciones realizadas en la ciudad de Pucallpa.

De la muestra de 138 usuarios de tarjetas de crédito y débito de las entidades bancarias y financieras de la ciudad de Pucallpa, 15 personas que representa el 10.87% de los encuestados respondieron que no existe ningún grado de relación del fraude por falta de protección de la contraseña de las tarjetas en operaciones realizadas en la ciudad de Pucallpa.

Figura 18



CAPÍTULO V

DISCUSIÓN DE RESULTADOS

5.1 CONTRASTACIÓN DE LOS RESULTADOS DEL TRABAJO DE CAMPO CON LOS REFERENTES BIBLIOGRAFICOS DE LAS BASES TEORICAS.

De los resultados conseguidos se deduce que existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa, tal como se desprende de las figuras 1, 4, 7.

De acuerdo con (Javato Martín, 2013), señala que:

La generalización del uso de las tarjetas de crédito y débito ha provocado un fuerte incremento de delitos relacionados con ellas. Concretamente ha disparado los fraudes en su utilización. Estos fraudes se pueden cometer tanto en los pagos efectuados en comercios, en los realizados a través de redes telemáticas, así como en la extracción ilegítima de dinero en cajeros automáticos. También ha multiplicado las conductas de falsificación de estos medios de pago.

En ese contexto existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.

Por ente que existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.

De acuerdo con el objetivo específico se establece que existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

5.2 CONTRASTACIÓN DE LA HIPÓTESIS GENERAL EN BASE A LA PRUEBA DE HIPÓTESIS

De la contrastación de la hipótesis general en base a la prueba de hipótesis se infiere que existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa.

CONCLUSIONES

De los resultados conseguidos se infiere que existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa, por lo que se concluye:

- Que Existe grado de relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa. Por ello el 74,64% de la muestra señala que existe relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas, frente a un 2,17% que señala lo contrario.
- Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa. De allí que el 78,99% de la muestra señala que existe relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero frente a un 8,70% que señala lo contrario.
- Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa. De Ahí que el 72,46% señala que existe relación significativa frente a un 7,25% que señala lo contrario.

SUGERENCIAS

De las conclusiones se infiere que existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de débito y crédito en el entorno virtual de los negocios en la ciudad de Pucallpa, por lo que se sugiere:

- Que las entidades bancarias y financieras deben de garantizar y generar confianza en sus clientes mitigando el fraude por robo de datos en cajeros automáticos con sistemas de detección modernas ante la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.
- Que los clientes de tarjetas de créditos y débitos deben obtener un protocolo de seguridad de las entidades bancarias y financieras para evitar el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.
- Que los clientes de tarjetas de créditos y débitos deben tener aseguradas las tarjetas para evitar las pérdidas por sustracción de fondos, que es una modalidad del fraude más usual del ciberdelito la clonación de tarjetas por operaciones comerciales ante la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.

REFERENCIAS BIBLIOGRÁFICAS

- Abanto Alejo, R. (2020). *La clonación de tarjetas de crédito y la responsabilidad civil de la entidad financiera Los Olivos año 2020*. Lima:
<https://hdl.handle.net/11537/25054>.
- Arroyo Morales, A. (2020). *Metodología de la investigación en las ciencias empresariales*. Cusco: Universidad Nacional San Antonio Abad del Cusco.
- Aruquipa Machicado, R. (2019). *Auditoria Forense sobre tarjetas clonadas caso: Banco Unión*. La Paz: <http://repositorio.umsa.bo/xmlui/handle/123456789/20998>.
- AUDITOL. (2020). *Guía de auditoría forense del fraude con tarjetas de crédito y débito*. Bogotá: www.auditool.org.
- Aures García, Á. A., & Boza Velez, P. E. (2018). *Implantación de tecnología EMV en la Red ATM Banbif*. Lima: <http://repositorio.usil.edu.pe/handle/USIL/3983>.
- Carrasco Díaz, S. (2007). *Metodología de la investigación*. Lima: Editorial San Marcos.
- Carrasco Diaz, S. (2007). *Metodologia de la investigacion cientifica*. Lima: Editorial San Marcos.
- Castro Acosta, R. (2013). *Responsabilidad en los fraudes con tarjetas de pago*. Laguna: Universidad de la Laguna.
- Del Pino Duran, M., Nieves Peñala, K. E., & Masias Pancorbo, M. (2019). *La asimetría de la información y su incidencia en el nivel de endeudamiento de los usuarios de tarjetas de crédito del Banco Internacional del Perú – Tienda Real Plaza Cusco año 2018*. Cusco: <http://repositorio.uandina.edu.pe/handle/UAC/3762>.

- Durango Rodriguez, N., Roldan, L. M., Rincon, L. M., & Taborda, D. A. (2017). *Clonación de tarjetas de crédito*. Antioquia:
<https://dspace.tdea.edu.co/handle/tda/163>.
- García Donayre, E. F., & Enero Santos, R. E. (2018). *Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú*. Lima: <https://hdl.handle.net/20.500.12867/1230>.
- Gariboldi, G. (1999). *Comercio electrónico conceptos y reflexiones básicas*. Buenos Aires: Instituto para integración de America Latina.
- Hernández Mejía, D. A. (2018). *El funcionamiento del comercio electrónico, categorías seguridad para usuarios y demografía de usos habituales*. Ecatepec de Morelos: <http://ri.uaemex.mx/bitstream/handle/20.500.11799/95210/TESIS-COMERCIO-ELECTRONICO.-Definitivo...pdf?sequence=1&isAllowed=y>.
- Javato Martín, A. M. (2013). *Las tarjetas de crédito y débito*. Salamanca España: <http://catedraseguridad.usal.es/node/11>.
- Linares Galvan, J. E. (2020). *Control interno en la prevención y detección del fraude corporativo*. Bogota: <https://www.javeriana.edu.co/personales/hbermude/Audire/jelg2.pdf>.
- Martinez Hernández, L. M. (2014). *Virtualidad, ciberespacio y comunidades virtuales*. Red Durango de Investigadores Educativos, A.C.: Mexico.
- Millan. (1989). *Declaración de la responsabilidad del Auditor interno*. Madrid España.
- Montoya Guillén, F. A. (2018). *Regulación expresa del delito informático de clonación de tarjetas-sede DIVINDAT, 2017*. Lima: <https://hdl.handle.net/20.500.12692/39776>.

- Muñoz Luque, J. M., Murcia Torres, A., & De los Rios Castro, N. (2019). *Propuesta de un modelo de inteligencia de negocios para la selección y planificación de una plataforma digital presentada a las sociedades especializadas en depositos y pagos electronicos (SEDPE)*. Mexico: <http://hdl.handle.net/10823/1813>.
- Palomino Ochoa, J. J., Dominguez Cuellar, C., Palomino Ochoa, R. L., & Torres Soria, I. (2021). *Métodos de investigación y praxis cuantitativa*. Huancayo: Corporación Atlas SAC.
- Rodriguez Bravo, O. M. (2020). *Analisis de los delitos informaticos en base a la alteración y modificación mediante transferencia electronica en modadlidad tarjeta de crédito*. GUayaquil:
<http://repositorio.ulvr.edu.ec/bitstream/44000/4146/1/T-ULVR-3450.pdf>.
- Suarez Beltrán, S. A., & Perea Obregón, M. S. (2018). *Auditoria forense como herramienta en la detección del fraude financiero*. Bogota:
<http://hdl.handle.net/20.500.12494/7980>.
- Superintendencia de Banca y Seguros, S. (2020). *¿Como evitar ser victimas de fraudes financieros?* Lima: <https://www.sbs.gob.pe/portals/3/educacion-financiera-pdf/cartilla%20adultos%204%20-%20MENSAJES%20Y%20LLAMADAS%20SOSPECHOSAS.pdf>.
- UNIREMINGTON. (2016). *Teoria general del control*. Medellin: Corporación universitaria Remington.
- Vásquez Rivera, M. E. (2019). *Implementación de E-Commerce en una empresa que se dedica a la compra-venta de muebles para baño ubicada en el oriente de la ciudad de México*. México:

[https://tesis.ipn.mx/bitstream/handle/123456789/27991/CP2019%20V375M.pdf?
sequence=1&isAllowed=y.](https://tesis.ipn.mx/bitstream/handle/123456789/27991/CP2019%20V375M.pdf?sequence=1&isAllowed=y)

ANEXOS

Anexo 1: Matriz de consistencia

TITULO: TRANSACCIONES EN EL MERCADO ELECTRONICO Y EL FRAUDE CON TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLE	DIMENSIONES	METODOLOGIA		
<p>Problema General: ¿Cuál es la relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa?</p> <p>Problemas específicos:</p> <ul style="list-style-type: none"> - ¿Cuál es la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa? - ¿Cuál es la relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa? - ¿Cuál es la relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa? 	<p>Objetivo general: Analizar la relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.</p> <p>Objetivos Específicos:</p> <ul style="list-style-type: none"> - Analizar la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa. - Determinar la relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa. - Establecer la relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa. 	<p>Hipótesis general Existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.</p> <p>Hipótesis específicas:</p> <ul style="list-style-type: none"> - Existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa. - Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa. - Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa. 	<p align="center">TRANSACCIONES EN EL MERCADO ELECTRONICO</p>	Fraude de robo de datos en cajeros automáticos	<p>Investigación básica</p> <p>Enfoque cuantitativo</p> <p>Alcance relacional</p>		
				Fraude telefónico		<p>Manipulación de tarjetas atascadas en Cajeros Automáticos</p> <p>Obtención de datos confidenciales clave toquen digital</p>	<p>Diseño no experimental</p> <p>Transversal</p> <p>Población</p>
				Fraude de clonación de tarjetas			
			<p align="center">FRAUDE CON TARJETAS DE CRÉDITO Y DÉBITO</p>	<p>Manipulación de tarjetas atascadas en Cajeros Automáticos</p> <p>Obtención de datos confidenciales clave toquen digital</p>	<p>Diseño no experimental</p> <p>Transversal</p> <p>Población</p>		
						<p>Protección de clave de tarjeta y POS</p>	<p>Muestra</p> <p>Instrumentos:</p> <p>Encuesta</p> <p>Cuestionario</p> <p>Estadística inferencial</p>



Anexo 03

UNIVERSIDAD NACIONAL DE UCAYALI
ESCUELA PROFESIONAL DE CONTABILIDAD

ENCUESTA: Tesis “**TRANSACCIONES EN EL MERCADO ELECTRONICO Y EL FRAUDE CON TARJETAS DE CRÉDITO Y DÉBITO EN EL ENTORNO VIRTUAL DE LOS NEGOCIOS DE LA CIUDAD DE PUCALLPA**”; marcar las alternativas que considere pertinentes con una (X):

Ítems	1	2	3
	Alto	Bajo	Ninguna

Ítems	1	2	3
I DIMENSION: Robo de datos en Cajeros Automáticos			
1. Existe grado de relación entre las transacciones en el mercado electrónico y el fraude con tarjetas de crédito y débito en el entorno virtual de los negocios en la ciudad de Pucallpa.			
2. Existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas en la ciudad de Pucallpa.			
3. Existe grado relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación			

de tarjetas atascadas en la ciudad de Pucallpa.			
II. DIMENSIÓN: Fraudes telefónicos			
4. Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.			
5. Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.			
6. Existe grado de relación entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero en la ciudad de Pucallpa.			
III. DIMENSION: Fraude clonación de tarjetas			
7. Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.			
8. Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el momento de la transacción en la ciudad de Pucallpa.			
9. Existe grado de relación entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS en el			

momento de la transacción en la ciudad de Pucallpa.			
IV. DIMENSION: Manipulación de tarjetas atascadas en Cajeros Automáticos			
10. Existe grado de relación entre el fraude por colaboración de particulares en la manipulación de tarjetas atascadas en los cajeros automáticos.			
11. Existe grado de relación entre el fraude por la falta de previsión de la exposición de clave por falta de descripción en la ciudad de Pucallpa.			
12. Existe grado de relación entre el fraude por falta de previsión de objetos sobrepuestos en los cajeros automáticos de la ciudad de Pucallpa.			
V. DIMENSIÓN: Obtención de datos confidenciales clave toquen digital			
13. Existe relación entre el fraude por obtención de datos confidenciales de clave de toquen digital por simulación de llamadas de criminales.			
14. Existe relación entre el fraude por obtención de datos confidenciales de clave de cajeros por simulación de llamadas de criminales.			
15. Existe relación entre el fraude por obtención de datos confidenciales de contraseña de la banca por simulación de llamadas de criminales tarjetas de habientes en la ciudad de Pucallpa.			
VI. DIMENSIÓN: Protección de clave de tarjeta y POS.			
16. Existe grado de relación del fraude por falta de protección de clave de tarjetas en la ciudad de Pucallpa.			

17. Existe grado de relación del fraude por falta de solicitud en el acto de POS por operaciones con tarjeta en la ciudad de Pucallpa.			
18. Existe grado de relación del fraude por falta de protección de la contraseña de las tarjetas en operaciones realizadas en la ciudad de Pucallpa.			