UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

ESCUELA PROFESIONAL DE DERECHO

PROYECTO DE TESIS

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

PRESENTADO POR:

BACH. CATAÑO BARDALES TERESA LUCRECIA.

BACH. PANDURO AREVALO LINDA LUCERO.

PARA OBTENER EL TITULO PROFESIONAL DE ABOGADO

ASESOR

…….....

PUCALLPA – PERU

2022

RESUMEN

La investigación titulada “El delito informático y su incidencia en las operaciones financieras en los bancos de la provincia coronel portillo- ucayali 2022”, y se plantea como objetivo de investigación Determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de coronel portillo- Ucayali 2022, es una investigación cuantitativa, de diseño no experimental, de nivel correlacional, en la que se planteó el siguiente problema de investigación ¿ De qué manera el delito informático incide en las operaciones financieras en los bancos de la provincia de coronel portillo – Ucayali 2022?, teniendo como hipótesis de investigación El delito de información incide significativamente en las operaciones facinerosas en los bancos de la provincia de coronel portillo- Ucayali 2022 y las sus variables de estudio son delito informatico y operaciones financieras en la que se tiene como dimensiones de estudios acceso a una base de datos, uso ilegal de la información, operación Phishing, gestión de riesgo, otorgamiento de crédito.

En la que se tiene como muestra de estudio a 263 personas bancarizadas de 18 a 70 años, a los que se aplicaran los cuestionarios de investigación para conocer sus opiniones respecto al tema investigado y para la preba de hipótesis se seguirán seis pasos en la que se utilizara herramientas estadísticas descriptivas con un nivel de confiabilidad del 95%.

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

ABSTRACT

The research entitled "Computer crime and its impact on financial operations in the banks of the Colonel Portillo-ucayali province 2022", and the research objective is to determine how the crime of information affects financial operations in the banks of the province. province of coronel portillo- Ucayali 2022, is a quantitative research, of non-experimental design, of correlational level, in which the following research problem was raised: How does computer crime affect financial operations in banks in the province? of colonel portillo - Ucayali 2022?, having as research hypothesis the crime of information has a significant impact on criminal operations in the banks of the province of colonel portillo- Ucayali 2022 and its study variables are computer crime and financial operations in which It has as dimensions of studies access to a database, illegal use of the to information, Phishing operations, risk management, credit granting.

In which the study sample is 263 banked people from 18 to 70 years old, to whom the research questionnaires will be applied to know their opinions regarding the investigated topic and for the hypothesis test, six steps will be followed in which will use descriptive statistical tools with a reliability level of 95%.

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

I. PLANTEAMIENTO DEL PROBLEMA

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

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

Esta situación va en aumento, ya que las instituciones financieras no dan la garantía y /o protección a sus clientes ya que a diario escuchamos o vemos en los medios de comunicación que una banda cibernética con modalidades y equipos modernos irrumpen en sus sistemas vulnerando la información de

sus clientes de los cuales esto no se hacen cargo al momento de reembolsar las perdices económicas de sus clientes.

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

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

1.1. Problema General.

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

1.1.1. Problemas Específicos.

- ¿ En qué medida el delito informático incide en las operación phishing de los bancos de la provincia de coronel portillo- Ucayali 2022?.
- ¿ En qué medida el delito informático se relaciona con la gestión de riesgos en los bancos de la provincia de coronel portillo – Ucayali 2022?.
- ¿ En qué medida el delito informático incide en la vulnerabilidad de los créditos otorgados por los bancos de la provincia de coronel portillo- Ucayali 2022?

II. JUSTIFICACION DEL PROYECTO

2.1. Justificación teórica

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

2.2. Justificación practica

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

2.3. Justificación metodológica

La presenta investigación utilizara buscará conocer la problemática en cuanto a las variables de investigación mediante proceso que conllevaran a la recopilación y análisis de información, en cuanto al delito informático y su incidencia en las operaciones financieras de los bancos de la provincia de coronel portillo- Ucayali 2022, para lo cual utilizaremos las herramientas necesarias de indagación, con el fin plantear estrategias de solución a la problemática en estudio.

La investigación utilizara los conocimientos científicos con el propósito de crear nuevos conocimientos sobre el delito informático.

2.4. Importancia

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

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

2.5. Delimitación

Delimitación temporal

En la presente investigación se usará información que corresponda al periodo 2022

Delimitación teórica

La investigación que se realiza alcanzará únicamente al delito informático y las operaciones financieras de los bancos.

2.6. Viabilidad de la investigación

Este proyecto será viable porque contamos con todos los recursos necesarios para efectuar el estudio, tales como materiales, economías y disponibilidad de tiempo, entusiasmo para llevarla a cabo.

III. HIPOTESIS

3.1. Hipótesis general.

El delito de información incide significativamente en las operaciones facinerosas en los bancos de la provincia de coronel Portillo- Ucayali 2022..

3.1.1. Hipótesis específicas.

- Existe incidencia entre el delito de información y las operaciones

phishing en los bancos de la provincia de coronel Portillo – Ucayali 2022.

- Existe relación entre el delito informático y la gestión de riesgos en los bancos de la provincia de coronel Portillo – Ucayali 2022
- Existe incidencia entre el delito de información y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de coronel Portillo – Ucayali 2022

IV. OBJETIVO

4.1. Objetivo general

Determinar como el delito de información incide en las operaciones financieras de los bancos en la provincia de coronel portillo- Ucayali 2022.

4.1.1. Objetivo especifico

- Determinar en qué medida el delito informático incide en las operaciones Phishing de los bancos de la provincia de coronel portillo- Ucayali 2022..
- Determinar en qué mediada el delito informático tiene relación cona gestión de riesgos de los bancos de la provincia de coronel portillo.
- Determinar en qué media el delito informático incide en vulnerabilidad de los créditos otorgados por los bancos de la provincia de coronel portillo- Ucayali 2022

V. ANTECEDENTES

5.1. Antecedentes internacionales.

Martínez (2015), en su estudio titulado “La responsabilidad bancaria frente a los delitos informático”, de la universidad Andina Simón bolívar- Sede Ecuador- Quito, en la que concluyo; La SB y la FG, emitieron resoluciones en el año 2011, mediante las cuales se exigió a las entidades bancarias realizar la reintegración a sus clientes, que sufrieron las consecuencias de

los delitos informáticos. Al emitir las resoluciones se empleó argumento constitucional, civil y derecho del consumidor; en el área constitucional se recalcó que las entidades financieras brindan asistencia pública, en el área civil se refirió a la obligación objetiva. Sin embargo, quedaron interrogantes respecto a la legalidad, así también si realmente las entidades bancarias brindan una asistencia pública o si es un contrato banco-cliente en el cual puede imponerse una responsabilidad objetiva, Las modalidades más comunes de estos delitos a nivel nacional son el pharming y el phishing, integrados en el COIP como delitos. Tanto los bancos como sus clientes son víctimas ante estos delitos cibernéticos de apropiación ilegal, los cuales se llevan a cabo por personas que normalmente no pertenecen a los bancos, pese a ello teniendo en cuenta el riesgo operacional son las llamadas a reducir estos riesgos, otorgando la información tecnológica apropiada que haga que los servicios por internet sean confiables, La obligación civil de los bancos frente a sus clientes en los delitos cibernéticos surge de una obligación contractual de banca en línea, lo cual excluye a terceros u otros usuarios que no habiendo efectuado ningún contrato con el banco utilizan estos servicios.

Rodríguez (2015), en su estudio titulada “Responsabilidad bancaria frente al phishing” de la universidad nacional de Colombia, en la que se concluyó. La simplicidad y bienestar que las negociaciones electrónicas abastecen al consumidor y a las empresas cada día es mayor, lo que hace presentir que hacia un futuro no muy lejano será el medio por el cual de forma muy natural el consumidor efectúe todas sus transacciones económicas. Lo que denota que todos los involucrados en estos tipos de negocios, perciben grandes ganancias de ellos, simplificación en la contabilidad de las empresas, simpleza de la transacción del consumidor y la entidad bancaria por la disminución de los costes humanos y físicos del negocio realizado. Es así,

que todos son beneficiarios de la simplicidad que otorgan las negociaciones, ya que, es mucho más fácil y más barato movilizar electrones que mover papel. Pese a ello, la utilización de estas plataformas virtuales, genera una variedad de peligros que cada vez se torna más incontrolable, tal que cada vez es menos sorprendente cuando se escucha en las noticias de algún hacker que logra desbloquear los sistemas de seguridad informáticas y militares del estado. Y si ellos son frágiles, es evidente que el sistema respecto a los negocios de comercio vía internet, tienen mayor grado de vulnerabilidad, estando más dispuestos a ser agredidos. Existe una amplia gama de posibles agresiones desde aquellas en contra de los servidores para impedir que accedan al servicio y los robos de información y autenticidad usados por los usuarios para dar el consentimiento de su transacción, con el cual posteriormente lograr engañar al proveedor y suplantar al cliente. Siendo las entidades bancarias muy sensibles a estas actividades.

5.2. Antecedentes nacionales.

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

igual que los policías, Para determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad, se encontró que la deontología tecnológica que afecta la competitividad de los operadores de justicia influye en la impropia determinación del tipo penal y en la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

De la cruz (2021), en su estudio titulada " Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la Provincia de Huaura -Huacho 2018", de la Universidad José Faustino Sánchez Carrión - Perú, al que se llegó a las siguientes conclusiones; : Según los resultados obtenidos mediante las encuestas un 86% considera que, el sistema financiero y bancario frente a los fraudes, no brinda garantía a sus clientes en los tiempos actual, Después de efectuar un análisis un 100% considera que, frente a las transacciones fraudulentas debe ser el sistema bancario y financiero quien debe responder a favor de sus clientes, aun cuando el cliente no contrate un Seguro, para un 94% considera que, las operaciones financiadas por internet se relacionan de manera significativa con la responsabilidad civil de los bancos, Las posiciones teóricas y estadísticas asumen que un 79% considera que, no es justificatorio que los bancos no asuman la gestión de los riesgos en la atención a los clientes mediante la banca por internet. .

5.3. Antecedentes locales.

(Marín y Santa maría, 2021), en su estudio titulada "El ciberdelito de redes delictivas a escala global a entidades gubernamentales y la responsabilidad del órgano de control interno en una municipalidad de la región de Ucayali, año 2020", de la Universidad nacional de Ucayali - Perú y se llegó a las siguientes conclusiones; Se concluye que hay una estrecha relación entre los

riesgos tecnológicos y la implementación de un área de prevención con un auditor interno antifraude de los fondos de las municipalidades Distritales o Provinciales. De los resultados obtenidos el 92,00% está completamente de acuerdo que los riesgos tecnológicos tienen relación la implementación de un área de prevención con un auditor interno antifraude de los fondos, el 1,10% no sabe al respecto. - Se concluye que hay una estrecha relación entre los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos de las municipalidades Distritales o Provinciales. De los resultados obtenidos el 68,20% está completamente de acuerdo los riesgos de robo de identidad de funcionarios y la prevención de los sistemas informáticos, el 1,10% no sabe al respecto. - Se concluye que hay una estrecha relación entre los riesgos informáticos en el desvió de fondos y la obtención de una seguridad razonable del control interno de las municipalidades Distritales o Provinciales. De los resultados obtenidos el 89,70% está completamente de acuerdo que los riesgos informáticos en el desvió de fondos y la obtención de una seguridad razonable del control interno, el 1,10% no sabe al respecto.

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

VI. MARCO TEORICO

6.1. Delito informatico

Vilca (2018), “Acción, típica, antijuridica y culpable que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónico y redes de internet” (p.21)

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

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

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

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

Tipifica los delitos informáticos en variedad de modalidades como: Ataques contra sistemas y datos informáticos, Usurpación de la identidad, Distribución de imágenes de agresiones sexuales contra menores, Estafas a través de Internet, Intrusión en servicios financieros en línea, Difusión de virus, Botnets (redes de equipos infectados controlados por usuarios remotos) y el Phishing (adquisición fraudulenta de información personal confidencia (Alarcón y Barrera 2017, p.71)

El delito informático es perpetrado por el uso de la computadora a través de redes y sistemas de información sistematizada. Independiente del propósito y finalidad deseada por parte del criminal o delincuente informático. Es importante resaltar que en el delito informático existen dentro del marco

jurídico la acción de los sujetos que intervienen en ellas por ello tipifican dos que son sujeto activo y sujeto pasivo, de acuerdo a ello se conceptúa de la siguiente forma (Alarcón y Barrera 2017, p.72)

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

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. Este nuevo mundo virtual lleno de datos, que se ha construido a partir del uso de las Tics, corre el peligro de ser alterado mediante conductas antisociales y delictivas. Éste fenómeno ha sido advertido por juristas y legisladores quienes, han realizado algunos esfuerzos por establecer los denominados delitos informáticos (Nando 1999, p. 96)

Ruiz (2016), “como la apropiación de la información y la intimidad personal en las redes sociales, y debe considerárselo acto antijurídico y ser causa de sanción y considerárselo como delitos informáticos, ya que afectan la privacidad de una persona, y al colectivo en general” (p. 9)

6.1.1. Modalidades del delito informatico

> Se entiende como criminalidad informática aquel conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es el ingreso no autorizado a computadoras, correos o sistemas de datas mediante clave de acceso, la destrucción o daña a base de datos y programas, estos delitos tienen la características que solo pueden ser cometidas por medios de sistemas informático. (Hancco E. 2017, p. 30)

Hancco E. (2017), “El delito informático en un sentido amplio, es decir comprende todas aquellas conductas que las TIC son el objetivo o el medio de ejecución del delito, la comisión de estos actos delictuosos plantea la especialización de los individuos que las cometen”. (p. 30)

6.1.1.1. Fraudes

> Los sujetos buscan alguna ventaja patrimonial, la norma regula como “procurar un provecho ilícito”, la conducta implica “el diseño, alteración, borrado, supresión, clonación o alteración del sistema informático a efectos de mantener en error a la víctima y en esa circunstancia aprovecharse ilícitamente, esta modalidad se da por ejemplo cuando se clonan páginas web de entidades financieras a efectos de obtener los datos financieros de la víctima y con dichos datos sustraer sumas de dinero y/o realizar compras en perjuicio de la víctima, por otro lado, témenos (Hancco 2017, p. 30)

6.1.1.2. Manipulacion de datos de entrada

> Este tipo de delito consiste en la sustracción de códigos y claves que la víctima utiliza para el ingreso a almacenamiento de datos, acceso a programas, etc., la característica de este delito es que la obtención de esta información se da cuando la víctima accede a determinado programa, sistema, página web, donde previamente se ha acondicionado el sistema para la sustracción y/o manipulación de la información, esto puede suceder cuando se clona la página web de una entidad financiera a efectos de obtener los datos de las tarjetas de crédito de la víctima. (Hancco 2017, p.32)

6.1.1.3. Manipulacion de datos de salida

> Hancco (2017) ,En este tipo de delito incide en la información

o datos que la víctima obtiene del sistema informático esta falsa información permite a los delincuentes aprovecharse del error en que se encuentra la víctima a efecto de conseguir determinados beneficios. (p.32)

6.1.1.4. Manipulacion de programas

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

Hancco (2017), “Una de las formas es el uso de troyanos que son programas que ingresan bajo un disfraz de un programa solicitado, sin embargo, en el sistema de la víctima empieza a ejecutar el programa oculto que por lo general busca el control remoto del ordenador de la víctima” (p.33)

6.1.2. Caracteristicas de los delitos informáticos

De acuerdo a Blossiers (2018), las características de los delitos informativo son las siguientes.

- Conductas criminales de cuello blanco
- acciones ocupacionales
- acciones de oportunidad
- provocan perdidas económicas
- muchos casos y pocas denuncias
- Proliferación continua
- Ilícitos de impunidad ante la ley
- Delitos que genera robos por medio de tarjeta de crédito
- Sistemas impersonales

- Fraudes que son deficientes de equiparar (Blossiers 2018, p.28).

6.2. Operaciones financieras

Son en primer término, aquellas celebradas por las entidades de crédito para captar y colocar recursos de manera profesional esto es permanente y masiva, por cuanto corresponden al objeto social propia de estas instituciones financieras. La clasificación más aceptada en América Latina divide a las operaciones financieras en dos grandes grupos: las primeras llamadas fundamentales o típicas, que corresponde en el fondo a la realización de un negocio de crédito y las otras denominadas complementarias o accesorias, agrupan todas las demás que prestan las entidades bancarias. (Arteaga y Choquehuanca 2017, p. 45)

6.2.1. Riesgos operacional

Este peligro surge, cuando coexiste la eventualidad de error o perjuicio, a causa de los procesos de aceptación, proceso, realización y acumulación de los informes, como a las personas encargadas de su administración. Las diferencias respecto al tema de protección son altamente significativas, ya que las entidades bancarias pueden padecer agresiones en cuanto a métodos o efectos. Este mal uso del peligro operacional también se puede aparecer del lado del consumidor, o por métodos inadecuados de la banca en line. (De la cruz 2021, p.27.

6.2.2. Banca por internet

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

telefonía celular. (De la cruz 2021, p. 40).

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

De la cruz (2021), Por lo cual, se define a este acuerdo como el que concedes recurrir a las prestaciones y productos utilizables de una institución bancaria vía online.(p.41).

6.2.3. Operaciones Phishing

Los phishers simulan pertenecer a entidades bancarias de reconocido prestigio y solicitan a los cibernavegantes datos de tarjetas de crédito o claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web, con una apariencia similar a la de la web original. En este caso, es el propio incauto internauta quien proporciona los datos requeridos, permitiendo al autor del ilícito lograr un beneficio económico ilegitimo (Mori 2019, p.91).

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

El phishing es un tipo de engaño creado por hackers, pero en este

caso con fines delictivos, para obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. Generalmente, el engaño se basa en la ignorancia del usuario, porque ingresa a un sitio que presume real, auténtico o que es el legal (Rodríguez 2009, p.297)

6.2.4. Gestion de riesgo

Utiliza las tácticas que consiente efectuar el Sistema de Control Interno en las instituciones públicas privadas trasgrediendo en la Gestión de Riesgos, formando definiciones, procedimientos y métodos expresados por los entes de control para corregir o mejorar los riesgos. (De la cruz 2021, p. 49)

6.2.5. Otorgamiento de crédito

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

6.3. Definición de términos básicos

Banca por internet: De la cruz (2021), Por lo cual, se define a este acuerdo como el que concedes recurrir a las prestaciones y productos utilizables de una institución bancaria vía online.(p.41)

Delito informático: Vilca (2018), “Acción, típica, antijuridica y culpable que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónico y redes de internet” (p.21)

Fraudes: implica “el diseño, alteración, borrado, supresión, clonación o alteración del sistema informático a efectos de mantener en error a la víctima y en esa circunstancia aprovecharse ilícitamente, esta modalidad se da por ejemplo cuando se clonan páginas web de entidades financieras a efectos de

obtener los datos financieros de la víctima (Hancco 2017, p. 30)

Gestión de riesgo: Utiliza las tácticas que consiente efectuar el Sistema de Control Interno en las instituciones públicas privadas trasgrediendo en la Gestión de Riesgos, formando definiciones, procedimientos y métodos expresados por los entes de control para corregir o mejorar los riesgos. (De la cruz 2021, p. 49)

Manipulación de datos de entrada: consiste en la sustracción de códigos y claves que la víctima utiliza para el ingreso a almacenamiento de datos, acceso a programas, etc., (Hancco 2017,p.32)

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

Operación financiera: Arteaga y Choquehuanca (2017), "aquellas celebradas por las entidades de crédito para captar y colocar recursos de manera profesional esto es permanente y masiva, por cuanto corresponden al objeto social propia de estas instituciones financieras" (p.45)

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

Phishing: Los phishers simulan pertenecer a entidades bancarias de reconocido prestigio y solicitan a los cibernavegantes datos de tarjetas de crédito o claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web, con una apariencia similar a la de la web original. En este caso, es el propio incauto internauta quien proporciona los datos requeridos, permitiendo al autor del ilícito lograr

un beneficio económico ilegitimo (Mori 2019, p.91)

Uso indebido de información: si el individuo actuó con el fin de obtener un beneficio económico, será reprimió con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

7. METODOLOGIA

7.1. Método general

Como método general se utilizará el método inductivo y deductivo.

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

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

7.1.1. Diseño de la investigación

El diseño de la investigación fue el diseño No Experimental, debió a que no se manipulara ninguna de las variables de estudio, solo se observara.

Para Sampieri, Fernández y Baptista (2014), "La investigación No experimental son estudios que se realizan sin la manipulación deliberada de las variables en estudio y en los que solo se observan los fenómenos en su ambiente natural para analizarlos" (p. 185)

7.1.2. Tipo de la investigación

La investigación será de tipo básico, porque se partira de una hipótesis, utilizara la observación, para contrastar las hipótesis y corroborar la teoría existentes, la investigación básica también es conocida como la investigación pura la cual lleva los conocimientos básicos a la realidad. .

En el tiempo; será transversal porque lo realizaremos durante el año 2022

De acuerdo Hernández (2014), precisa que "la investigación transversal

recolecta datos en un solo momento, es como una retrato de lo que acontece"(p. 150)

7.1.3. Nivel de la investigación

La presente investigación será correlacional porque estudiaremos la relación entre las variables de estudio.

Enfoque de la investigación

El enfoque que se utilizará en la investigación será el cuantitativo para la recolección, procedimiento y análisis de la información.

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

7.2. Lugar de estudio

La investigación se efectuará en la Provincia de Coronel Portillo, Ucayali a 104 a 2072 msnm

7.3. Población y muestra

7.3.1. Población

Según García (2012) "la población es el conjunto mayor de objetos, que tienen al menos una característica común, cuyo estudio nos interesa o acerca de los cuales se desea información" (p. 56).

Para determinar la población, se tomó como fuente a Ipsos Perú (2021) que nos indica que más de 8.9 millones de peruanos están bancarizados lo que representa el 52% de la población de 18 a 70 años, de cual se toma como población para la presente investigación a 836 bancarizados de entre 18 a 70 personas, con el fin de realizar el presente estudio.

7.3.2. Muestra

Para Tamayo y Tamayo (2012),indica que "es el grupo de personas que se toma de la población, para investigar un fenómeno estadístico" (p. 363).

Formula:

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

Donde:

N = Población o Universo
Z = Nivel de confianza
e = Margen de error
p = Probabilidad de Éxito
q = Probabilidad de Fracaso
n = Muestra Inicial

Cálculo de la muestra

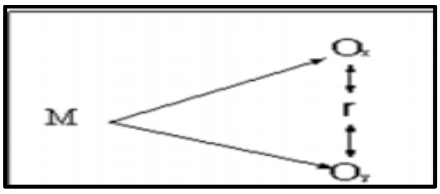
N	=	952
Z	=	1.96
e	=	0.05
p	=	0.50
q	=	0.50
n	=	274

Fuente; *Elaboración propia*

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

7.4. Descripción de los métodos materiales, equipos

7.4.1. Diseño de muestreo



M= personas bancarizadas de entre 18 a 70

Ox= Delito informatico

r= Relación existente entre las dos variables

Oy= Operaciones finacieras

7.4.2. Descripción de los materiales y equipos

Recursos materiales: Computadora, Impresora, Papel bond, Tinta para impresora, Correctores, Lapiceros, Lápices.

Recursos humanos: Asesor, encuestador, investigador

7.4.3. Descripción de las variables de estudio

Variable independiente : Delito Informático

Dimensiones

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

Variable dependiente: Operaciones Financieras
Dimensiones

Y1:Ambito social
Y2:Ambito jurídico
Y3: Ámbito político

7.4.3.1. Operacionalización de variables

Variables	Definición conceptual	Dimensiones	Indicadores	Técnica
VARIABLES Delito Informático	Acción, típica, antijuridica y culpable que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónico y redes de internet" (p.21)	**X1:** Acceso a una base de datos	**X1.1** Vulnerabilidad de los datos	cuestionario
			X1.2. vulnerabilidad de la información personal	
		X2: Uso ilegal de la información	**X2.1**. Suplantación de identidad	
VARIABLE Operaciones Financieras	Arteaga y Choquehuanca (2017), "aquellas celebradas por las entidades de crédito para captar y colocar recursos de manera profesional esto es permanente y masiva, por cuanto corresponden al objeto social propia de estas instituciones financieras" (p.45)	**Y1:** Operaciones Phishing	**Y1.1.** Captación mediante internet	cuestionario
		Y2: Gestión de riesgos	**Y2.1**.Monitoreo de procesos **Y2.2.** Estrategias de control	
		Y3: Otorgamiento de Créditos	**Y3.1.** Desembolsos de prestamos **Y3.2.** Otorgamientos de tarjetas de crédito	

Tabla 1: Operacionalización de variables
Fuente: Elaboración propia

7.4.4. Aplicación de prueba estadística inferencial

Para la prueba de hipótesis se utilizará el estadístico SPSS ; con la que conoceremos la relación entre las variables de estudio; así mismo, seguiremos 6 pasos en la que plantearemos la hipótesis nula y alterna, el nivel de significancia, función de prueba, reglas de decisión, calculo y conclusión.

7.4. Tabla de recolección de datos.

Variables	Recolección de datos	Procesamiento de datos	Instrumento
Delito Informático	Para el proceso de recolección de datos se utilizaremos el cuestionario con la que obtendremos los datos respecto a las variables de estudio.	Se procesarán los datos recolectados en tablas estadísticas, ya que, al ser una investigación cuantitativa se trabajará por porcentajes en la cual se seguirá el siguiente procedimiento. En primer lugar, se iniciará buscando información bibliógrafa fica para ampliar los conocimientos en cuanto a las variables de estudio. Segundo se procederá a elaborar los instrumentos de investigación, Tercero se efectuar la aplicación del instrumento de investigación, Finalmente se realizará la prueba de hipótesis y plantearemos la discusión, conclusión y recomendación de la investigación..	Encuesta
Operaciones Financieras			

Tabla 2: recolección de datos
Fuente: Elaboración propia

8. CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	2022				
	Jun	Jul	Agt.	Set	Agt.
1. Elección del tema					
2. Revisión de bibliográfica					
3. Formulación de la matriz de consistencia					
4. Redacción del marco teórico					
5. Elaboración del proyecto de investigación					
6. Aprobación del proyecto de investigación					
7. Recolección de datos					
8. Procesamiento de datos					
9. Redacción del informe					
10. Presentación del informe					
11. Sustentación de la tesis					

Tabla 3: Cronograma de actividad
Fuente: Elaboración propia.

9. PRESUPUESTO Y FINANCIAMIENTO

9.1. Presupuesto

Descripción del rubro	Cantidad	Valor Unitario (S/.)	Valor Total (S/.)
Bienes:			
Laptop	01 unidades	2500.00	2500.00
Lapiceros	01 docenas	1.00	12.00
Borrador	4 unidades	1.00	4.00
Mascarillas descartables	1 caja	15.00	15.00
Servicios:			
Impresiones	01 millares	0.20	200.00
Copias	1/2 millar	0.03	15.00
Internet	5 meses	60.00	300.00
Movilidad			300.00
Otros			200.00
TOTAL			**4246.00**

Tabla 4: Presupuesto
Fuente: Elaboración propia.

9.2. Financiamiento

La presente investigación será financiada por el investigador.

10. BIBLIOGRAFICA

Alarcón Ariza, D. A., y Barrera Barón, J. A. (2017). Uso de internet y delito informático en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016. Escuela de Posgrado. Lima, Perú: Universidad Privada Norbert Wiener.

Ander-Egg, E. (1995). Técnicas de investigación social (Vol. 24). Buenos Aires: Lumen.

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

Blossiers Mazzini, J. J. (2018). El delito informático y su incidencia en la empresa bancaria. Escuela Universitaria de Posgrado. Lima, Perú: Universidad Nacional Federico Villareal.- Perú

Carrasco, S. (2007). Metodología de la investigación científica. Pautas metodológicas para elaborar un proyecto de investigación.

De la cruz (2021), en su estudio titulada " Operaciones financiadas por internet y su relación con la responsabilidad civil de los bancos en la Provincia de Huaura -Huacho 2018", de la Universidad José Faustino Sánchez Carrión - Perú

Hancco E. (2017), "La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017" de la universidad nacional de san Agustín – Perú

Hernández, R, Fernández, C. y Baptista, P. (2014). Metodología de la Investigación. Colombia: Editorial Mc Graw. Hill.

Marín y Santa maría . (2021), en su estudio titulada "El ciberdelito de redes delictivas a escala global a entidades gubernamentales y la responsabilidad

del órgano de control interno en una municipalidad de la región de Ucayali, año 2020", de la Universidad nacional de Ucayali – Perú

Martínez (2015), en su estudio titulado "La responsabilidad bancaria frente a los delitos informático", de la universidad Andina Simón bolívar- Sede Ecuador-Quito

Mori (2019) en su estudio titulada "Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, Periodo 2008 al 2012", de la Universidad Nacional Federico Villarreal, Perú,

NANDO, LEFORT, Víctor, (1999) El lavado de dinero, nuevo problema para el campo jurídico, 2ª edición Editorial Trillas, México,

Rodríguez (2015), en su estudio titulada "Responsabilidad bancaria frente al phishing" de la universidad nacional de Colombia

Ruiz C. (2016) "análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos" de la Universidad nacional de Loja – ecuador.

Solorzano L. (2018) "Los hackers: "delito informático frente al código penal peruano" de la universidad Nacional Santiago Antúnez de Mayolo – Perú.

Tamayo y Tamayo, M. (2012). Técnicas de Investigación. 2ª Edición México: Editorial Mc Graw Hill.

Vilca Aira, G. L. (2018). Los hackers: delito informático frente al código penal peruano. Facultad de Derecho y Ciencias Políticas. Anchas, Perú: Universidad Nacional Santiago Antúnez de Mayolo

11. ANEXOS: MATRIZ DE CONSISTENCIA

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

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
PROBLEMA GENERAL	Objetivo General	Hipótesis General	**DELTO INFORMATICO**	**X1:** Acceso a una base de datos	**X1.1** Vulnerabilidad de los datos	• **Sistema de métodos** **Método general:** Inductivo - deductivo • **Tipo de investigación:** Básica **En el tiempo:** Transversal. **Nivel de la investigación:** Correlacional **Diseño de la investigación:** No Experimental **Enfoque de la investigación:** cuantitativa • **Población y muestra** **Población:** 836 personas bancarizadas de 18 a 70 años **Muestra:**263 • **Técnicas recolección de datos** **Técnicas:** Encuesta **Instrumentos:** cuestionario, **Técnicas de procesamiento de datos:** Se procederá a analizar los datos mediante la herramienta de EXCEL, los resultados se analizarán vía estadística descriptiva y para el contraste de hipótesis se utilizará el Spss versión 21 y se seguirán. 6 pasos**.**
¿De qué manera el delito informático incide en las operaciones financieras en los bancos de la provincia de coronel portillo – Ucayali 2022?	Determinar como el delito de información incide en las operaciones financieras en los bancos de la provincia de coronel portillo- Ucayali 2022	El delito de información incide significativamente en las operaciones facinerosas en los bancos de la provincia de coronel portillo- Ucayali 2022			**X1.2.** vulnerabilidad de la información personal	
				X2: Uso ilegal de la información	**X2.1**. Suplantación	
Problemas específicos	**Objetivos específicos**	**Hipótesis especificas**	**OPERACIONES FIANCIERAS**	**Y1:** Operaciones Phishing	**Y1.1.** Captación mediante internet	
¿En qué medida el delito informático incide en las operación phishing de los bancos en la provincia de coronel portillo- Ucayali 2022?.	Determinar en qué medida el delito informático incide en las operaciones Phishing de los bancos en la provincia de coronel portillo- Ucayali 2022	Existe incidencia entre el delito de información y las operaciones phishing de los bancos en la provincia de coronel portillo – Ucayali 2022				
¿En qué medida el delito informático se relaciona con la gestión de riesgos de los bancos de la provincia de coronel portillo – Ucayali 2022 ?	Determinar en qué mediada el delito informático tiene relación cona gestión de riesgos de los bancos de la provincia de coronel portillo.	Existe relación entre el delito informático y la gestión de riesgos de los bancos de la provincia de coronel portillo.		**Y2:** Gestión de riesgos	**Y2.1**.Monitoreo de procesos **Y2.2.** Estrategias de control	
¿en qué medida el delito informático incide en la vulnerabilidad de los créditos otorgados por los bancos de la provincia de coronel portillo- Ucayali 2022?	Determinar en qué media el delito informático incide en vulnerabilidad de los créditos otorgados por los bancos de la provincia de coronel portillo- Ucayali 2022	Existe incidencia entre el delito de información y la vulnerabilidad en los créditos otorgados por los bancos de la provincia de coronel portillo – Ucayali 2022		**Y3:** Otorgamiento de Créditos	**Y3.1.** Desembolsos de prestamos **Y3.2.** Otorgamientos de tarjetas de crédito	