UNIVERSIDAD PARTICULAR DE CHICLAYO

FACULTAD DE DERECHO Y EDUCACIÓN

ESCUELA DERECHO

TESIS PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

"El Skimming como modalidad de delito informáticos en la ley 30096, y los niveles de inseguridad ciudadana en la provincia de Chiclayo Región Lambayeque"

Autor:

CESAR IVAN ESPINOZA BRAVO

Asesor:

Mg. MAURO ALINDOR YRIGOÍN SOTO

https://orcid.org/0009-0003-7899-4615

LINEA DE INVESTIGACIÓN

Derecho Público y Privado.

Derecho Penal, procesal penal, sistema de penas, causa y formas del fenómeno criminal

Pimentel, Perú - 2024

UNIVERSIDAD DE CHICLAYO

ACTA DE CONTROL DE ORIGINALIDAD DE LA INVESTIGACIÓN

Yo, **Enrique Rodas Ramírez**, Decano de la Facultad de Derecho y Educación ha realizado el debido control de originalidad de la investigación, el mismo que está dentro de los porcentajes establecidos para el nivel de pregrado, según la Directiva de Similitud vigente en la UDCH; además certifico que la versión que hace entrega es la versión final del informe presentado por el bachiller: **ESPINOZA BRAVO CESAR IVAN.**

Titulado: "**EL SKIMMING COMO MODALIDAD DE DELITO INFORMÁTICOS EN LA LEY 30096, Y LOS NIVELES DE INSEGURIDAD CIUDADANA EN LA PROVINCIA DE CHICLAYO REGIÓN LAMBAYEQUE**".

Elaborado por el estudiante, **ESPINOZA BRAVO CESAR IVAN.** Se deja constancia que la investigación antes indicada tiene un índice de similitud del 15% verificable en el reporte final del análisis de originalidad mediante el software de similitud **TURNITIN.**

Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre el nivel de similitud de productos acreditables de investigación vigente.

Pimentel, 17 de octubre de 2024.

Dr. Enrique Rodas Ramírez
DECANO

EL SKIMMING COMO MODALIDAD DE DELITO INFORMÁTICOS EN LA LEY 30096, Y LOS NIVELES DE INSEGURIDAD CIUDADANA EN LA PROVINCIA DE CHICLAYO REGIÓN LAMBAYEQUE

Tesis presentada por el bachiller ESPINOZA BRAVO CESAR IVAN, de la facultad de Derecho y Educación de la Universidad Particular de Chiclayo, para optar el Título profesional de Abogado

Bachiller:

Espinoza Bravo Cesar Ivan

Asesor:

Mg. Yrigoin Soto Mauro Alindor

Aprobado por:

Dr. Enrique Rojas Ramirez
Presidente

Dr. Javier Soriano Diaz Diaz
Secretario

Mg. Jorge Pedro Flores Santa Cruz
Vocal

DEDICATORIA

A Dios, por su infinita gracia en mi vida

A mi familia por ser mi fortaleza para continuar esforzándome en mi crecimiento profesional.

AGRADECIMIENTO

A la Universidad de Chiclayo, gran institución educativa

A sus Autoridades y docentes por su profesionalismo

RESUMEN

La investigación respecto a los delitos informáticos es motivada desde el enfoque penal, pues ante el avance tecnológico se hace necesario que se analicen los tipos penales que se van presentando en esta era de modernidad, así se desarrolló el tema “El Skimming como modalidad de delito informáticos en la ley 30096, y los niveles de inseguridad ciudadana en la provincia de Chiclayo Región Lambayeque”, con el objetivo de determinar la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo en el año 2022; la metodología fue con un tipo de investigación básica descriptiva, y enfoque cualitativo, la técnica de la entrevista ha tenido como resultado que los entrevistados aporten ideas de seguridad ciudadana sobre la incidencia del delito skimming, que viene atravesando en la provincia de Chiclayo. El resultado que se obtiene de los entrevistados en sus opiniones plantean, que si hay una afectación a la inseguridad ciudadana, con incremento de ilícito del Skimming, al poner en riesgo constantemente el robo de identidad en sus transacciones bancarias, y comerciales por parte de un sujeto activo; se concluye que la usurpación de identidad (skimmng) identificada en el sistema penal según la ley 30096, es un ciberdelito, que se ejecuta robando los datos de identidad de otra persona mediante sistema electrónico en las tarjetas de crédito o débito, con el fin de un beneficio económico. Ningún ciudadano se encuentra seguro de sufrir en algún momento esta situación de que te roben tu identidad para realizar transacciones fraudulentas perjudicándote económicamente, por lo tanto, si afecta la seguridad ciudadana.

Palabras claves: delito informático, skimming, seguridad ciudadana.

ABSTRACT

The research regarding computer crimes is motivated from the criminal approach, because in the face of technological progress it is necessary to analyze the criminal types that are being presented in this era of modernity, thus the topic "Skimming as a modality of computer crime in law 30096, and the levels of citizen insecurity in the province of Chiclayo Lambayeque Region" was developed. with the aim of determining the incidence of Skimming as a modality of computer crime indicated in Law 30096, which generates citizen insecurity in the province of Chiclayo in the year 2022; the methodology was with a type of descriptive basic research, and qualitative approach, the interview technique has resulted in the interviewees providing ideas of citizen security on the incidence of skimming crime, which has been going through in the province of Chiclayo. The result obtained from the interviewees in their opinions states that there is an impact on citizen insecurity, with an increase in the illicit of Skimming, by constantly putting at risk identity theft in their banking and commercial transactions by an active subject; It is concluded that the identity theft (SKIMNG) identified in the criminal system according to Law 30096, is a cybercrime, which is carried out by stealing the identity data of another person through an electronic system on credit or debit cards, in order to obtain an economic benefit. No citizen is sure to suffer at some point from this situation of having your identity stolen to carry out fraudulent transactions, harming you economically, therefore, it does affect citizen security.

Keywords: computer crime, skimming, citizen security.

INDICE

Índice de tablas

I.- INTRODUCCIÓN

La presente problemática denota la importancia de investigar los delitos informáticos, de manera específica el Skimming, aplicando las descripciones teóricas y legislación enfocada a la ciberlincuencia y con la finalidad de establecer parámetros respecto a similares o distintos criterios que se encuentren el desarrollo de la presente investigación; asimismo, el trabajo que se desarrollará es importante de manera práctica en tanto, se recabarán opiniones y puntos de vista de diversos colaboradores que analizarán la problemática referida los delitos informáticos, datos que serán analizados de manera metodológica, aplicando los distintos sistemas de recopilación de información, para que estas sean tratadas como tal. (Espinoza C. V., 2022)

De acuerdo al organismo internacional “Comisión económica para América Latina y el Caribe CEPAL (2022), En América Latina, se observa una carencia de legislación suficiente en materia de delitos informáticos, lo que genera una gran diversidad de delitos y bienes jurídicos que necesitan protección. Esto incluye delitos contra el patrimonio, propiedad (física o intelectual), personas (intimidad, imagen y domicilio), y hacienda pública, los cuales han sido abordados por normativas diversas, como reformas de códigos penales, leyes especiales y hasta leyes de comercio electrónico, lo que evidencia la necesidad de una regulación más integral y coherente.

En América, los países buscan soluciones legislativas para combatir los fenómenos criminales informáticos, adoptando diferentes enfoques. La mayoría ha reformado sus códigos penales (Argentina, Bolivia, Costa Rica, Guatemala, México, Paraguay, Perú), mientras que otros han creado leyes específicas (Brasil, Chile, Colombia, Venezuela). Ecuador ha utilizado una ley de comercio electrónico para introducir normas penales, y Uruguay solo cuenta con una ley de Protección del Derecho de Autor.

En países sin reformas, se intenta reinterpretar la normativa vigente para incluir delitos informáticos, lo que puede aumentar el riesgo de impunidad debido a la falta de tipificación específica. Esto puede llevar a situaciones en las que los delitos informáticos no cumplan con los requisitos mínimos de delitos "clásicos", como la posesión física en el hurto, lo que puede dificultar su persecución y

sanción, y destacando la importancia del principio de legalidad en materia penal "nullum crimen nulla poena sine lege"". (CEPAL,2022)

Nuestro país, no es ajeno, la problemática de la existencia de bandas delictivas dedicadas a la clonación de tarjetas. Perjudicando económicamente a muchas personas que hoy en día es común que cuenten con una o más tarjetas bancarias adscritas al sistema financiero y comercial del país; por ello el Estado tiene que estar obligados en la búsqueda de mecanismos de control y sancionadores con la finalidad de proteger a los usuarios, sancionar penalmente a quienes cometen estos delitos informáticos; que además colocan en riesgo la economía de una sociedad.

El Ministerio Público (2022) mediante el observatorio de criminalidad, informa que en los últimos años se viene evidenciando el incremento de los delitos informáticos, en diversas modalidades, siendo que los datos obtenidos en sus registros indican la existencia de 21,687 denuncias, y que por cada año que va transcurriendo su incremento es progresivo, llegando a incrementar un 42%. Ante ello promulgaron la Ley N°30096 - Ley de Delitos Informáticos, y las recomendaciones adoptadas del Convenio de Ciberdelincuencia donde el Estado se encuentra suscrito).

La provincia de Chiclayo, viene padeciendo de diversos tipos de delitos informáticos entre los más resaltantes es el skiming, cometidos por integrantes en su mayoría extranjeros, siendo este delito el que representa en un 20.2 % que se viene cometiendo mediante utilizando el engaño a ciudadanos con mensajería fraudulenta donde hacen revelación de confidencial información por voluntad propia. Posteriormente, estas acciones ocasionan una merma de clientes y proveedores generando niveles de desconfianza. (Defensoría del Pueblo, 2024)

Las causas del incremento de delitos informáticos se presentan por que la sanción penal que presenta la ley 30096 es relativamente inferior a otras sanciones penales que delitos contra el patrimonio. Las consecuencias jurídicas deberán ser modificar la ley que norma el tipo penal de los delitos informáticos a fin de encontrar que disminuya el índice delictivo.

Nuestro estudio se vincula con el Objetivo noveno de Desarrollo Sostenible, que busca fomentar la industria, la innovación y la infraestructura, ya que la implementación de tecnologías de información y comunicación es crucial para lograr un desarrollo sostenible y fortalecer a las comunidades en diversos países. Para alcanzar este objetivo en 2030, es fundamental brindar apoyo a los Países Menos Avanzados (PMA) y realizar inversiones en tecnologías avanzadas.

La formulación del problema es: ¿Cuál es la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo?

Los problemas específicos serán: a) ¿De qué manera se desarrolla el ilícito informático de Skimming según la Ley 30096 en la legislación penal peruana? b) ¿Cómo se encuentran descritos los aspectos generales y penales de seguridad ciudadana según nuestra norma legal peruana? y c) Cual es el análisis de la situación problemática de inseguridad ciudadana producto del inicito de Skimming como modalidad de delito informáticos señalado en la ley 30096?

En esta investigación, se pretende investigar, se encuentra desarrollada en un problema que viven muchas ciudades del mundo, donde los avances tecnológicos en el sector económico y social se vienen desarrollando de manera diaria pues la tecnología avanza día a día, y pegado a ella las ideas o actos de la delincuencia. En la actualidad ya no es necesario realizar transacciones comerciales con dinero en efectivo o emisión de cheques, pues las tarjetas de crédito representan el dinero llamado “plástico”, mediante una tarjeta de crédito que es expuesta constantemente en los bancos, agentes bancarios, centros comerciales, etc.

La justificación práctica, se desarrollará en la indagación respecto a la ciberdelincuencia conforman una fuerte corriente delictiva de última generación que perturba la seguridad ciudadana afectando los aspectos económicos y patrimoniales de la sociedad que se ven afectados, así también las instituciones y empresa privada.

La justificación teórica, se presentará en el desarrollo de las bases teóricas de las categorías como son delitos informáticos, la seguridad ciudadana, el ilícito de

Skimming análisis de la ley N.º 30096, los mismos que permitirán tener ubicado dentro de la literatura de la doctrina al investigador al momento de desarrollar la tesis.

Respecto a la justificación metodológica, se hace uso del formato de desarrollo de investigación propuesto por la Universidad de Chiclayo, considerando los tipos de estudio, el método y las técnicas para la recopilación de información practica desde formulación de problemas y objetivos, cuya finalidad es resolver los problemas planteados.

El objetivo general es: determinar la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo en el año 2022; siendo los objetivos específicos a) desarrollar el ilícito informático de Skimming según la Ley 30096 en la legislación penal peruana, b) describir los aspectos generales y penales de seguridad ciudadana según nuestra norma legal peruana y c) analizar la situación problemática de inseguridad ciudadana producto del inicito de Skimming como modalidad de delito informáticos señalado en la ley 30096.

III.- DESARROLLO

De acuerdo Sierra (2022) en su investigación denominada “Percepción de Inseguridad de los Ciudadanos de Bucaramanga y Floridablanca”, teniendo como objetivo principal: Determinar cuál es el nivel de conocimiento de los ciudadanos respecto a la inseguridad en Bucaramanga y Floridablanca, aplicando un desarrollo metodológico de tipo cuantitativa, la investigadora llego a la siguiente conclusión: Aquellos comportamientos delictivos descritos en la investigación son los más frecuentes y suceden en los espacios donde hay mayor inseguridad afectando su calidad de percepción y vida de inseguridad.

Se evidencia que el autor ha logrado determinar factores positivos de la lucha o enfrentamiento en Bucaramanga respecto a los ciberdelitos y también resalta el desarrollo de conectividad de MinTIC, de la misma forma brinda recomendaciones precisas respecto a la ciberseguridad que se encuentran regulados.

Según Padilla (2022), en su investigación denominada “Inseguridad ciudadana y delitos de mayor connotación social: formas y extensiones del temor a la delincuencia en Chile”, teniendo como objetivo: la exploración y análisis de la inseguridad ciudadana de chile ante la delincuencia, específicamente la que se vincula a los ilícitos de grande connotación social, aplicando una metodología de tipo cuantitativa, los investigadores han llegado a la siguiente conclusión: que no se debe subestimar la importancia de los delitos contra la propiedad, ya que afectan la sensación de seguridad y generan pérdidas económicas significativas.

El autor interpreta que los delitos informáticos en Chile van de manera escalonada, donde el Estado asume más responsabilidad por la protección de Gobierno, considerando como delitos de primera dimensión, y los delitos informáticos cometidos contra ciudadanos comunes y corrientes son considerados como de primera subdimensión, por lo que la seguridad ciudadana debe ser favorecida mediante campañas de sensibilización, de manera urgente se requiere el aumento de su cobertura y difusión, puesto que, es un mecanismo que disuade al usuario para adoptar medidas de cuidado y siguiendo el protocolo establecido.

Molinos (2020), en su investigación “El Fraude Informático y Telemático: Perspectiva Penal Valladolid”, cuya finalidad fue establecer un enfoque globalizado en relación a tipos penales que están sostenidos en el artículo 248.2 a) y c) de la Ley Orgánica 10/1995, la metodología fue descriptiva, de análisis documental para analizar el comprendido del art. 248 del CP. Se determina que este delito comparte similitudes con la estafa tradicional en varios aspectos, aunque no cumple con todos los elementos característicos de esta, como el engaño, el error, la disposición del patrimonio por parte del sujeto activo, el daño a la víctima, la intención de obtener beneficio económico y la relación causal entre estos requisitos.

El autor, analiza los delitos informáticos desde la estructura de la norma penal, analizando el tipo penal establecidos en la Ley Orgánica 10/1995; los tipos penales de la estafa informática y la telemática; con la utilización de tarjetas de crédito o datos que se combinan en información comercial por cualquier usurario, haciendo una diferencia dependiendo del uso de tarjeta d crédito que se usa para cometer el ilícito, pues las tarjetas consideradas de disponible abierto, las ciber tarjetas y las tarjetas prepago entre otras se excluyen de este tipo penal.

Dentro de los antecedentes nacionales, tenemos a Ponce (2022), en su tesis “La clonación de tarjetas de créditos y débitos, su implicancia como delito informático en el Perú”, el objetivo que examina la eficacia de la legislación actual para abordar el creciente problema de la clonación de tarjetas de créditos y débitos en el Perú. Mediante un enfoque cualitativo descriptivo y análisis de datos textuales, el autor concluye que es necesario crear una nueva ley específica para delitos informáticos, en lugar de modificar la legislación existente, que ya ha sido objeto de cambios y podría generar confusión. Se mencionan la Ley N.º 30096 y su modificatoria, la Ley N.º 30171, como referentes en la materia.

El autor considera que este acto ilícito es muy considerable y peligros al sistema económico (comercial y financiero), motivado por la globalización, el sujeto tiene el objetivo de sustracción de dinero ajeno. Sosteniendo como normas legales, La Ley N.º 30177. Y su regulación con la Ley N.º 30096.

Carrera (2023), en la tesis denominada “Fundamentos jurídicos para concentrar el phishing como agravante en el artículo 11° de la Ley N.º30096 – Ley de delitos informáticos en el Perú”, teniendo como objetivo la determinación de fundamentos jurídicos que incorporen al phishing como agravante que establece el artículo 11° de Ley N.º 30096 –, aplicando una metodología de tipo básica de diseño no experimental, llegando a la siguiente conclusión: El delito del phishung es un delito contemporáneo que no está debidamente regulado y que al verse incrementado a pasos gigantes a nivel mundial se requiere que tenga una descripción en la legislación en concreto, para que de esa manera evite que sea impune y se apliquen las sanciones correspondientes.

El autor señala que la ley N.º30096 – Ley de ilícitos Informáticos, establece normas para diversas conductas delictivas en el ámbito cibernético, y a través de un análisis exhaustivo de cada artículo, se identificaron los bienes jurídicos que se ven afectados por estas acciones, utilizando los elementos del tipo penal.

Aldecoa (2020), en su investigación denominada “El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019”, teniendo como objetivo principal: establecer la forma donde las vías informáticas permiten el favorecimiento de actos ilícitos como suplantar identidad dentro del sistema financiero en Lima, 2019, aplicando un desarrollo metodológico de tipo cualitativa, llegando a la siguiente conclusión: El phishing es un mecanismo tecnológico aplicado para lograr la obtención de datos personales directos de la víctima usando herramientas tecnológicas para suplantar la identidad personal de un usuario del banco, favoreciendo así la perpetración del ilícito de suplantación de identidad.

El autor señala que se necesita una actualización inmediata de la norma Ley N° 30096, Ley de Delitos Informáticos, señala que en la actualidad se han incrementado los ilícitos informáticos en diversas modalidades contempladas en esta norma, aparte del incremento de la utilización de tecnologías de la indagación y la declaración merecen ser modificados y regulados de forma absoluta.

Ramos (2022) En su tesis "La regulación de las nuevas modalidades del delito informático en la ley N°30096 y su modificatoria, periodo 2020-2021",

Ramos (2022) examina la regulación de nuevas modalidades de delitos informáticos en la Ley Nro. 30096 y su modificatoria Ley Nro.30171. La investigación cualitativa y descriptiva, con un enfoque aplicado, involucró a 5 fiscales de Huaraz y analiza el ordenamiento jurídico peruano. Los resultados muestran que la falta de regulación específica de estas modalidades delictivas (Phishing, Smishing y Vishing) conduce a un aumento de estas conductas y a la impunidad. Se concluye que es necesario incorporar estas modalidades dentro de la Ley de Delitos Informáticos para sancionarlas adecuadamente.

Es evidente que el autor argumento que la Ley 30096 requiere de redacciones más concreta, puesto que, de ese modo, es viable que se garantice una persecución e identificación más idónea respecto a los ilícitos informáticos, para de ese modo cumplir con el objeto persecutor de la norma, donde las nuevas figuras de fraude informático no quedasen impunes.

A nivel local, se han citado las investigaciones de En su investigación "Ley de los delitos informáticos Nº30096 y su influencia en la población de Chiclayo en tiempos de Covid-19", Villanueva (2023) busca determinar el impacto de la Ley de delitos informáticos N°30096 en la población de Chiclayo durante la pandemia de Covid-19. Utilizando un enfoque cuantitativo descriptivo y correlacional, y un diseño no experimental transversal, los resultados muestran una correlación positiva moderada (r=0.403) entre los delitos informáticos y la integridad personal, con un nivel de significancia menor a 0.05, lo que indica una relación significativa entre ambos.

El autor hace referencia a que los ilícitos informáticos en los pobladores de Chiclayo, genera afectación a la moral, integridad física e integridad psíquica, que representan el 36.8%, recomendándoles que denuncien estos actos ya que la Ley 30096 tiene como finalidad erradicar este tipo de actos ilícitos.

Cumpa (2021), en su investigación “Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático”, teniendo como objetivo: identificar y analizar las modalidades actuales de cibercrímenes relacionadas con el fraude informático, con el fin de proponer su inclusión explícita en la ley especial, específicamente en el artículo 8 de la Ley N°30096, para mejorar la regulación y prevención de estos delitos, aplicando una metodología de diseño

cuantitativo de enfoque descriptivo, llegando a la siguiente conclusión: Ante las deficiencias y vacíos legales en la regulación de los ilícitos informáticos, especialmente en el fraude informático, que es un delito frecuente en la actualidad, es necesario agregar circunstancias de hecho específicas en el artículo 8 de la Ley 30096, para fortalecer la normativa y abordar de manera efectiva estas conductas delictivas.

El autor examina la Ley N° 30096, específicamente el artículo 8, y observa que solo se regula el fraude informático como delito informático contra el patrimonio, el cual castiga ilegítimamente la obtención de beneficios ilícitos, en contraste con la legislación argentina que incluye los delitos informáticos dentro de los delitos comunes, como el fraude informático en el artículo 173, inciso 16 del Código Penal Argentino.

Vásquez (2020) en su investigación “Factores de Riesgo de los Cibercrímenes Sociales y su Influencia en los Jóvenes de la Provincia de Chiclayo”, teniendo como objetivo general: Determinar cuáles son los factores de riesgo de los cibercrímenes sociales y cómo influyen en los jóvenes de la provincia de Chiclayo, aplicando una metodología de tipo cuantitativo y diseño descriptivo, llegando a la siguiente conclusión: para garantizar los derechos de las personas se ha desarrollado una política de seguridad informática contra los cibercrímenes.

El investigador pretende argumentar que las nuevas figuras ilícitas de los delitos informáticos se desarrollaron con el avance de la tecnología, convirtiéndose en un requerimiento para modificar los comportamientos repudiados por una Nación Democrática, la legislación que regula estos ilícitos es la Ley 30171 y 30096, que regula la misma.

Bernal (2022) en su tesis “Patrullaje cibernético y seguridad ciudadana en una entidad pública policial de Chiclayo, 2022”. El objetivo general fue investigar las causas de la ineficacia en el trabajo de los especialistas en administrar justicia (policías, fiscales y jueces) en la investigación y juzgamiento de ciberdelitos y hechos ilícitos relacionados. La metodología utilizada fue correlacional y cuantitativa, con un instrumento de encuesta y un informe basado en el método hipotético-deductivo. La investigación encontró una relación significativa entre el

patrullaje cibernético y el desarrollo de la seguridad ciudadana en la entidad policial estudiada, con un nivel de correlación alto (r = 0.860), similar a los hallazgos de Palella y Martins (2012).

Entendemos que el autor ha logrado demostrar el vínculo significativo que se presenta entre la planificación de seguridad con la evolución de la seguridad ciudadana en una institución estatal de la Policía que labora en Chiclayo, este vínculo se presenta basada en un valor correlacional de r=0.600., sugiriendo que la junta vecinal tiene que realizar una labor de forma conjunta con la comisaria con la finalidad disminuir los ilícitos cibernéticos.

En el desarrollo de las categorías se han ubicados desde lo general a lo especifico empezando por desarrollar los ciberdelitos, en la actualidad, no existe un consenso en cuanto al término adecuado para referirse a los delitos objeto de nuestro estudio; sin embargo, “cibercriminalidad” y “cibercrimen” hacen referencia a la corriente criminalística que investiga esta clase de delitos y sus diversos componentes. “Delito informático” es un término surgido en 1985, cuando se creía que la única forma de cometer estos delitos era desde una computadora, y —aún— no desde otros dispositivos electrónicos. Mientras que “ciberdelito” posee un concepto más amplio que comprende a los delitos informáticos tradicionales y a otros que irán apareciendo. (Elías, 2020)

Según la *Real Academia Española*, el término “ciber” está relacionado con las redes informáticas, mientras que el vocablo “ciberdelito” significa delito que se comete mediante el uso del internet. La expresión adecuada, en nuestra normativa encontramos el término “ciberdelincuencia”, art. 1º de la Ley N°30096, Ley de Delitos Informáticos, publicada el 23 de octubre del 2013. Ahí se señala que dicha ley tiene como finalidad “garantizar la lucha eficaz contra la ciberdelincuencia”. Sin embargo, a pesar de que usa dicho término en ese artículo, lleva como título general: Ley de Delitos Informáticos.

Existen dos posiciones doctrinarias al respecto: una corriente que señala que solo deben ser considerados ciberdelitos aquellos delitos en los que el uso de la tecnología sea indispensable y que no pueden ser cometidos de otra manera, y otra corriente que está de acuerdo con llamar ciberdelito a todos los delitos cometidos mediante las tecnologías de la información. (Torres, 2021)

Se cuenta con un concepto amplio de ciberdelitos, que según Tejada De La Fuente: señala que previamente se denominada ilícitos informáticos a merced de la preocupación del sistema penal al enfrentar los ilícitos perpetrados a través de herramientas tecnológicas o contra el sistema informático. Actualmente estos ilícitos han ocasionado una preocupación, puesto que tienen la posibilidad de cometerse a través de páginas web (particularmente a través de cualquier red social) equipos electrónicos de comunicación e información. (Delgado,2021).

Por su parte, *Barrio, (2021),* refiere: El ciberdelito es aquella infracción penal perpetrada en el ciberespacio, extendiéndose aquel espacio que se creó mediante un medio informático.

Esta categoría incluye una amplia gama de delitos informáticos, que se pueden clasificar en dos subgrupos: 1) delitos directamente relacionados con la informática: aquellos que atentan contra la integridad, confidencialidad y disponibilidad de equipos, datos o sistemas informáticos y 2) delitos tradicionales cometidos a través de medios electrónicos o digitales: incluye delitos como amenazas, coacciones, estafas, que son cometidos utilizando dispositivos electrónicos o digitales como medio para llevar a cabo la actividad delictiva.

Según Rivera (2022), define al delito informático a toda acción u omisión tipificada en la ley y sancionada con una pena realizada por una persona en el entorno de la informática que cause perjuicio a determinadas personas y beneficie ilícitamente al autor del delito. Asimismo, menciona algunos elementos del tipo penal que se deben considerar para identificar un delito de este tipo:

- El bien jurídico tutelado es la pureza de la técnica y el resguardo de los medios involucrados.
- El elemento subjetivo debe estar constituido por el dolo o culpa con que actúa la persona que comete el delito informático.
- El sujeto activo de este tipo de delitos es por lo general una persona con cierto nivel de inteligencia y educación, puede ser programador, analista de sistemas, analista de comunicaciones, supervisor, personal técnico y de mantenimiento, entre otros.
- Como sujeto pasivo frecuentemente se encuentra a las entidades bancadas, las cuales realizan movimientos mediante símbolos

electrónicos.

De igual manera, dicha autora indica que son acciones ocupacionales, va que muchas veces se realizan cuando el autor se encuentra en su centro de labores. Son acciones de oportunidad: el ciberdelincuente aprovecha la ocasión para su comisión. Provocan grandes pérdidas económicas a los afectados y beneficios a sus autores, incluso con números de más de cinco cifras. Presentan gran facilidad de comisión en el tiempo y el espacio, ya que pueden ser realizadas en un plazo mínimo y sin la necesidad de la presencia física de sus actores. En consecuencia, hay gran cantidad de casos; sin embargo, pocos de ellos son denunciados, pues existe dificultades para su comprobación debido a su carácter técnico. La gran mayoría de este tipo de delitos son de carácter doloso e intencional. Lamentablemente, estos delitos tienden a incrementarse por lo que es urgente su regulación nacional e internacional.

Los delitos informáticos son aquellas conductas ilícitas que se dan mediante las computadoras como instrumento o fin. Manifiesta también que los delitos informáticos son delitos de cuello blanco, ya que solo pueden ser cometidos por personas con conocimientos de informática. Ahora bien, respecto al término adecuado para definir este tipo de delitos, *Tejada De La Fuente*, indica que no existe una definición uniforme a nivel internacional; sin embargo, se entiende que ciberdelincuencia o criminalidad informática, en sentido amplio, sería todas las actividades delictivas relacionadas al empleo de las denominadas tecnologías de la información y de la comunicación (TIC), ya sea que dichas tecnologías sean el objeto de la acción ilícita o porque sean herramientas para la planificación o ejecución del delito. (Arce, 2020)

Según Fernández (2020), Los delitos informáticos han sido objeto de estudio en la doctrina desde la década de 1960, y su definición ha experimentado una evolución significativa en el transcurso de los años. En sus inicios, se entendían como actos que causaban daños físicos a infraestructuras informáticas. Posteriormente, en la década de 1970, se comenzaron a identificar conductas ilícitas relacionadas con la utilización indebida de sistemas informáticos. Durante la década de 1980, surgieron nuevas modalidades delictivas: ataques contra infraestructuras piraterías, críticas e ilícitas patentes. En aquella época, Callegari definió los ilícitos informáticos como a aquellos

realizados con ayuda de una técnica informática. Como referencia a ello un claro ejemplo en aquel periodo era la piratería de archivos multimedia y software, que se incrementan exponencialmente en las posteriores épocas. Al llegar el internet al hogar en el año de 1990 los ciberdelincuentes contaban con un medio nuevo y mecanismos para perpetrar aquellos actos ilícitos (Quintero, 2020)

En efecto, basándose en los conceptos previamente presentados, se han definido los ilícitos informáticos como un nuevo modo del desarrollo de los delitos a través del uso de un equipo tecnológico que tiene conexión a internet utilizando algún puerto que permite acceso a los archivos contenidos o al sistema

El siguiente cuadro presenta los principales delitos informáticos:

Categoría de Delito	Tipo de Delito
Ilícito contra la intimidad	Almacenar, modificar, revelar o difundir ilegalmente datos privados de personas.
Ilícito relativos al contenido	Difundir, de manera especial mediante Internet: pornografía infantil, afirmaciones racistas con informes incitadores a violencia.
Ilícito económicos, acceso no autorizado y sabotaje	La piratería, el sabotear informático y distribuir virus, espía informático, y la alteración y el fraude informáticos
Ilícito contra la propiedad intelectual	Ilícitos que afectan la protección jurídica de programas y bases de datos, derechos de autor y derechos afines.

Es necesario desarrollar la diferencia entre un ciberdelito y un delito común, para ello se tiene en cuenta a *Pérez, (2019),* un factor que diferencia un delito común de un ilícito informático es que el ilícito, para que se clasifique en el ámbito de los ciberdelitos, es que aquella conducta se perpetre con la intervención de algún sistema informático, ya que es su mayor particularidad.

Ahora bien, la diferencia entre delitos informáticos y los delitos comunes es que en los delitos informáticos siempre involucran el uso de “datos informáticos” y “sistemas informáticos”.

Asimismo, se considera que para la comisión de este tipo de delitos no solamente basta una computadora, sino que el uso del internet es indispensable. No existe ciberdelito que se pueda cometer sin el acceso a internet. Pero no todos los delitos cometidos mediante el uso de internet son ciberdelitos. Para considerarlos como tales, nos remitiremos exclusivamente a los tipos penales contenidos en la Ley N°30096, Ley de Delitos Informáticos.

Por otro lado, es necesaria una reclasificación de delitos informáticos o ciberdelitos, a merced de la existencia de que algunos de ellos no están dentro de la referida Ley Especial sino dentro del Código Penal, hemos determinado como ciberdelitos a ocho figuras ilícitas que están reguladas en la Ley Nº30096.

Respecto a las categorías de esta clasificación, *Miró (2020)* define: 1) Ciberataques de contenido: Se centran en la información o contenido transmitido a través de redes telemáticas, especialmente internet; 2) ciberataques puros: Son ataques que ocurren exclusivamente en el ciberespacio, sin equivalente en el espacio físico, y utilizan tecnologías de la información y comunicación (TIC) de manera innovadora y 3) ciberataques réplica: Son aquellos que utilizan el ciberespacio como medio para cometer delitos que ya existen en el espacio físico, pero se adaptan al entorno digital.

Según, *Vega (2022)*, menciona el Convenio de Budapest y clasifica los ciberdelitos en cuatro categorías:

1). Delitos contra la tecnología: atentan contra la confidencialidad, integridad o disponibilidad de la información, como daño informático o acceso ilícito a sistemas.

2). Delitos que utilizan la tecnología como medio: son delitos comunes que se cometen a través de sistemas informáticos, como fraude informático o falsificación de datos digitales.

3). Delitos relacionados con el contenido: incluyen la producción, posesión y distribución electrónica de material ilegal, como pornografía infantil.

4). Delitos relacionados con la propiedad intelectual: se refieren a la reproducción y difusión no autorizada de contenido protegido por derechos de autor en internet, como piratería.

De acuerdo con *Velasco Núñez*, existen tres tipos de ciberdelitos:

- En primer lugar, los delitos patrimoniales vinculados a la informática, cuya finalidad es obtener beneficios económicamente evaluables de terceras personas, como, por ejemplo, estafas Online, daños informáticos, publicidad engañosa o espionaje informático de secretos de empresa.
- En segundo lugar, atentados a la intimidad y privacidad, esto es, la llamada ciberdelincuencia intrusiva. Entre ellos podemos destacar las amenazas y coacciones informáticas, la distribución de material de pornografía infantil, descubrimiento y revelación de secretos o injurias y calumnias.
- En tercer lugar, ataques por medios informáticos a intereses supraindividuales con la finalidad de subvertir el orden político o de convivencia generalmente aceptado. Entre ellos, encontraríamos los delitos de descubrimiento y revelación de secretos relativos a la defensa nacional, el enaltecimiento del terrorismo o la captación de terroristas a través de medios de comunicación accesibles para el público.

Los ciberdelitos tienen un carácter pluriofensivo, ya que afectan múltiples bienes jurídicos de manera simultánea y concatenada. Por ejemplo, la información en general (almacenada, procesada y transmitida a través de sistemas automatizados) y otros bienes como la indemnidad sexual, la intimidad, entre otros. La información debe ser considerada no solo como un valor económico, sino también como un valor intrínseco de la persona, dada su importancia en el tráfico jurídico. Además, los sistemas que procesan o automatizan la información pueden afectar bienes tradicionales como el patrimonio (fraude informático), la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), la seguridad y fiabilidad del

tráfico jurídico probatorio (falsificación de datos o documentos probatorios), entre otros.

Los sujetos del delito, no se requiere una particularidad especial para considera el sujeto activo, de acuerdo a (Peña Cabrera Freyre, (2020): quien argumenta, es suficiente que el agente tenga determinada información propia de la informática para perpetrar este acto típico. Es posible admitir una autoría mediata, cuando una persona saca provecho de la buena fe de otra persona, del instrumento sin dolo, no tiene conocimiento de la acción que perpetra, accede de modo indebido a una basa o red de datos.

El menester hacer énfasis en que las personas jurídicas solo naturales no pueden ser consideradas como sujeto activo, no obstante, aquello implica que un sujeto jurídico sea pasible de efectos accesorios regularos en el art. 105 del Código Penal.

El sujeto pasivo, puede ser cualquier persona, (natural o jurídica). Según Villavicencio, (2014), quien cita a Gutiérrez, indica que: el sujeto pasivo es la persona jurídica, a razón del tráfico económico donde se desenvuelven sus acciones, ante esto representa los más afectados sectores por la criminalidad a través de computadoras. Se puede mencionar: las instituciones públicas, la industria de transformación, etc.

El "skimming" es un método ilícito que implica la extracción de datos de tarjetas de crédito o débito en un punto de venta, utilizando un dispositivo electrónico portátil llamado "skimmer", que lee la banda magnética de las tarjetas y transfiere la información a una computadora. Luego, los delincuentes descargan los datos en una tarjeta falsa con identidad diferente, lo que permite un uso indebido de la información y constituye un delito. (Espinoza C. V., 2022)

El autor Espinoza, tras un análisis detallado, concluye que el principal obstáculo para combatir el fraude informático es la complejidad para definir y sancionar este delito. La Ley N.º 30096 carece de la fuerza necesaria, y además, hay una falta de preparación entre los operadores de justicia y un presupuesto insuficiente para los organismos encargados de velar por la justicia. También se destaca la pasividad de las empresas emisoras de tarjetas, que no hacen lo

suficiente para proteger a sus usuarios, muchos de los cuales desconocen las medidas de seguridad.

Por lo tanto, es necesario seguir investigando y fortaleciendo la legislación peruana en materia de fraude informático, incluyendo la clonación de tarjetas de crédito y débito, para mejorar la intervención del Estado, el desarrollo de operaciones efectivas y el debido proceso para los acusados.

Es importante destacar que, antes de la Ley N.° 30096, los delitos informáticos estaban regulados en el Código Penal, pero carecían de independencia y eran insuficientes. El Legislador, inspirado en la Convención de Budapest de 2001, creó una ley especial que, aunque es un avance, sigue teniendo debilidades y vacíos legales, lo que beneficia a los delincuentes.

En resumen, el "skimming" o clonación consiste en robar información de la tarjeta de crédito durante una transacción comercial, al insertarla en un cajero automático, para luego clonarla y usarla fraudulentamente para adquirir bienes y servicios.

Para cometer este acto fraudulento, los delincuentes suelen utilizar dispositivos llamados skimmers para copiar la información almacenada en la banda magnética de las tarjetas de crédito. Este tipo de fraude electrónico es muy común en cajeros automáticos de entidades financieras en todo el mundo, debido a su fácil adquisición y rápida implementación, y genera buenos resultados para los cibercriminales.

En cuanto a la seguridad ciudadana en la provincia de Chiclayo, empezamos definiendo el concepto de seguridad ciudadana, que proviene del latín "sine cura" (sin cuidado, sin preocupación). La seguridad ha sido conceptualizada de diferentes maneras, incluyendo el mantenimiento del orden público, la no intervención violenta, la ausencia de violencia física y el derecho a la calidad de vida. Según Huerta (2019), la seguridad humana se define como la condición de vivir libre de temor y libre de necesidad.

El concepto de seguridad ciudadana es multifacético y abarca diversas dimensiones, por lo que es complejo de definir sin considerar todas sus facetas. Se puede describir como una situación social caracterizada por un ambiente de paz, armonía y convivencia entre los ciudadanos, que permite el ejercicio libre y pacífico de los derechos individuales, políticos y sociales, así como el funcionamiento normal de las instituciones.

La seguridad ciudadana engloba aspectos como la seguridad jurídica, social, defensa del principio de legalidad, protección del medio ambiente, lucha contra la pobreza, respeto a los derechos civiles y políticos, y condiciones económicas y sociales que permitan el desarrollo de las potencialidades individuales. Cuando las personas pueden realizar sus actividades sin temor a sufrir daños o menoscabos en cualquier ámbito, y pueden ejercer sus derechos y libertades de manera responsable y libre, se puede afirmar que existe seguridad ciudadana (Vizcarra, 2023)

La seguridad ciudadana tiene las siguientes características:

a) Incorpora el aspecto territorial, considerándolo una parte fundamental del bienestar de la población, en lugar de un objetivo en sí mismo, a diferencia de la seguridad nacional, b) se enfoca en la protección y promoción del bienestar de los ciudadanos en su entorno cotidiano, c) abarca aspectos como la seguridad jurídica, social, ambiental y económica d) se caracteriza por un ambiente de paz, armonía y convivencia entre los ciudadanos, d) permite el ejercicio libre y pacífico de los derechos individuales, políticos y sociales, e) incluye la protección del principio de legalidad, la lucha contra la pobreza y el respeto a los derechos civiles y políticos, f) Busca brindar condiciones para el desarrollo de las potencialidades individuales.

En cuanto a la seguridad pública, hay una diferencia notable: el mantenimiento del orden público se logra a través del ejercicio de las libertades, en lugar de mediante políticas punitivas. Los contextos sociales e institucionales relacionados con la violencia buscan describir las diversas manifestaciones violentas y delictivas en un sector determinado. Entre los factores que se destacan se encuentran:

a) Las condiciones sociales, como el deterioro y la desagregación social, económica y cultural, así como la presencia de agentes de riesgo como el alcohol, las drogas y las armas de fuego, que generan un ambiente propenso a la violencia y la delincuencia; b) las condiciones simbólico-culturales que validan prácticas y conductas ilícitas y corruptas en determinados sectores sociales, y que construyen identidades que favorecen estereotipos y legitiman formas de violencia contra ciertas poblaciones; c) las condiciones institucionales que caracterizan a un Estado débil e ineficiente en la aplicación de sus leyes y políticas.

Los conflictos que vulneran el orden público incluyen eventos políticos y sociales que alteran la paz y la tranquilidad, independientemente de si constituyen una infracción o delito. Esta categoría abarca protestas y movilizaciones violentas, desórdenes barriales y vecinales, y tumultos que violan normas básicas de convivencia ciudadana. Debido a sus motivaciones, características y respuestas institucionales únicas, estos conflictos requieren un análisis individualizado. Aunque afectan la seguridad ciudadana, no deben ser abordados junto con otros delitos desde una perspectiva criminológica.

Entre las teorías sobre seguridad ciudadana, se encuentra la Teoría de la disonancia cognitiva, que sugiere que la disonancia cognitiva puede frenar la expansión del crimen organizado. Esto se debe a que un segmento de la población muestra actitudes contradictorias, expresando desaprobación hacia las autoridades, pero simultáneamente mostrando apoyo o simpatía hacia figuras del crimen organizado, como sicarios, lugartenientes, narcotraficantes o capos (Albacerrín,2020).

III METODOLOGÍA

3.1.- Tipo de Investigación.

El tipo de investigación que se llevará a cabo es básica y descriptiva, ya que se centrará en analizar y describir contextos y situaciones específicas, con el fin de obtener una comprensión detallada y precisa de los fenómenos estudiados. La investigación será de tipo descriptivo, lo que permitirá examinar y caracterizar situaciones concretas de manera detallada. (Guevara, 2020)

3.2.- Diseño de investigación.

El diseño no experimental, él mismo que será dividido de acuerdo a la duración de la recolección de datos; estos serán: un diseño trasversal que será la recolección de datos dada en determinada y único momento, donde se describirán las categorías y sus enlaces de ese momento Sampieri (2021).

Investigación fenomenológica, pues se pretende comprender el significado de las experiencias relacionadas con el problema concreto. Mediante las entrevistas se exploran las experiencias subjetivas de los participantes de manera concreta u observaciones para descubrir las estructuras y pautas subyacentes de sus experiencias vividas. (Jain, 2023)

El enfoque de la investigación es cualitativo, lo que implica una descripción detallada y profunda de las circunstancias, eventos, personas, interacciones y comportamientos observados. Se incluyen las perspectivas y experiencias de los participantes, sus actitudes, creencias, pensamientos y reflexiones, tal como ellos las experimentan y expresan, sin interpretación del investigador. Este enfoque es descriptivo y se basa en la observación y descripción objetiva del comportamiento o situación estudiada, sin influir en ella de ninguna manera (Piña, 2023)

3.3.- Categorías, subcategorías y matriz de categorización.

Primera categoría: El Skimming como modalidad de delito informáticos en la ley 30096,

Segunda Categoría: Seguridad ciudadana en la provincia de Chiclayo.

Tabla 1: cuadro de Categorización

Categoría de estudio	Definición conceptual	Subcategoría
Categoría uno: El Skimming como modalidad de delito informáticos en la ley 30096,	Implica la obtención ilegal de información financiera de una tarjeta de crédito o débito en un punto de venta específico, utilizando un dispositivo electrónico portátil conocido como "skimmer", que es un lector de banda magnética capaz de extraer datos de las tarjetas plastificadas. Este dispositivo se instala en los cajeros automáticos, aprovechando su tecnología para capturar la información confidencial de las tarjetas (Espinoza C. V., 2022)	Definición del Skimming Orígenes del Skimming Los tipos de Skimming Clonación de tarjetas Antecedentes Consecuencias Delincuencia cibernética Sujetos Tipos
Categoría dos: Seguridad ciudadana	Es un concepto multifacético y profundamente arraigado en la sociedad y la política, que se define como un estado de equilibrio social caracterizado por la coexistencia pacífica, la armonía y la convivencia entre los ciudadanos. Este estado permite y promueve el ejercicio libre y pacífico de los derechos individuales, políticos y sociales, así como el funcionamiento óptimo de las instituciones públicas y privadas. (Estrada, 2015)	Realidad Seguridad Normas y participación Sistema de protección legal. Características

3.4.- Escenario de estudio.

Viene a ser, contexto físico, experimental o social en el que se realiza la investigación el cual será conformado con las características propias del Estudio a desarrollar, como es el contexto físico, social o experimental. (Palacios, 2020) . El escenario de estudio está conformado los Juzgados Penales (Poder judicial) de Chiclayo.

3.5.- Participantes

La población participante engloba a un conjunto de unidades, definida limitada y accesible, la cual está conformara para establecer una muestra en cumplimiento a una secuencia de criterios predeterminados. (Rodriguez, 2022)

Los participantes de la presente investigación, serán: 10 abogados profesionales de derecho penal quienes son colaboradoras en desarrollar la entrevista.

3.6.- Técnicas e instrumentos de recolección de datos.

Técnicas

Análisis documentales. Es la técnica más difundida en el proceso de investigación, se utiliza para analizar el contenido de ideas centradas en periódicos, revistas, libros, textos. Se podría decir que viene a ser la técnica precisa orientada a una descripción muy objetiva, ordenada y de calidad. En la presente investigación, se utilizará al momento de analizar las fuentes bibliográficas, sentencias, y materiales doctrinales que conforman el marco teórico. Los instrumentos son los textos, libros, separatas, que serán utilizados para obtener la doctrina y los antecedentes de estudio.

La observación. La observación es una de las principales metodologías utilizadas para investigar y comprender la sociedad, como destaca Ander-Egg. A pesar de ser un método antiguo, sigue siendo confiable y efectivo para recopilar datos y información, los cuales posteriormente son verificados y analizados para probar o refutar una hipótesis o alternativa de solución.

La entrevista

Es un instrumento técnico útil, en la investigación cualitativa, para lograr datos. Viene a ser una conversación que se propone un fin determinado distinto al simple hecho de conversar. (Gonzales, 2022)

Son métodos y instrumentos empleados para recolectar datos e información necesarios para probar o demostrar una hipótesis o alternativa de solución. En el contexto de una exploración cualitativa, se destacan técnicas de gran importancia, siendo la observación detallada su herramienta principal.

Se refiere a los métodos y herramientas utilizados para recopilar datos e información necesarios para validar una hipótesis, siendo la observación detallada una técnica fundamental en la exploración cualitativa.

3.7.- Procedimientos de recolección de datos e informaciones:

Mediante la observación, se recabaron datos visuales, como son la problemática existente en diferentes sectores financieros, comisarías, (denuncias realizadas por ciudadanos, poder judicial buscar audiencias respecto a los delitos que se estudian). (Inga, 2020)

Análisis documental, se seleccionaron libros, para revisar la bibliografía y jurisprudencia respecto al tema que se investiga, así mismo se buscaron tesis precedentes, para obtener los antecedentes de estudio que forman parte del desarrollo del presente tema. (Martinez, 2023)

En la entrevista, se recopilan las ideas y conocimientos trascritos en un documento plasmado con un formato, el mismo que luego se analizará, para hacer un estudio general de todas las entrevistas y se realizará una discusión de resultados, esto lo realizará el bachiller encargado de la investigación. (inga,2020)

Por tanto, se recolectará información necesaria, la cual ha sido procesada mediante un análisis, y procesados en el procesador de texto Microsoft Office, y las entrevistas serán analizadas, luego elaborar los cuadros y los resultados.

3.8.- Validez y confiabilidad

La validez y la confiabilidad dentro de la investigación, son ideas que se utilizan en la evaluación de la calidad de determinado estudio, utilizado de manera principal en investigaciones cuantitativas que permiten señalar los límites de un método, una técnica es medible de forma efectiva. (Narvaez, 2022)

Este aspecto esta desarrollado por el Especialista Magister o maestro al momento de revisar el instrumento y emitir su informa de valoración.

3.9.- Criterios de Rigor científico.

Rigor Científico: El rigor científico toma en cuenta la multidimensionalidad y flexibilidad de los aspectos conceptuales y metodológicos de la investigación realizada, con un público adecuado y libre de interpretar los resultados en función de sus propias necesidades y requerimientos de la investigación. (Durán, 2022)

Validez: La validez es el grado en que un instrumento mide la categoría que pretende evaluar. (Hernández, 2021)

Credibilidad: La credibilidad se logra cuando los resultados de la investigación son percibidos como "auténticos" o "verdaderos" por quienes participaron en la investigación y por quienes experimentaron o tuvieron contacto con el fenómeno que se estudia. (Castillo & Vásquez, 2003)

Confiabilidad: El concepto de confiabilidad, arraigado en la mente de la mayoría de los investigadores, continúa utilizándose dentro de la tradicional orientación epistemológica positivista, que superó en la segunda mitad del siglo XX. Esto plantea una contradicción porque la metodología cualitativa adopta un paradigma epistemológico postpositivista como base y postulado fundamental de las teorías del conocimiento y la ciencia. El propósito de la confiabilidad es garantizar que un investigador pueda seguir los mismos procedimientos y realizar el mismo estudio descrito previamente por otro investigador y llegar a los mismos resultados y conclusiones. (Miguélez, 2021)

3.10. – Aspectos éticos

Se mencionaron varios criterios, principios éticos y normas para guiar la investigación que implica a seres humanos, incluyendo:

a. Autonomía: La capacidad de las personas para tomar decisiones informadas y actuar de acuerdo con sus propios objetivos y valores, respetando las directrices y disposiciones establecidas.

b. Justicia: La imparcialidad en la distribución de obligaciones y derechos, lo que implica un discernimiento ético para evaluar si una acción es justa o no, considerando una perspectiva equitativa.

En otras palabras, se destacan la importancia de respetar la autonomía de los participantes en la investigación y garantizar la justicia en la distribución de beneficios y cargas, asegurando una evaluación ética rigurosa.

VI.- RESULTADOS

4.1.- De las entrevistas

Objetivo General: Determinar la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo en el año 2022.

¿Usted considera que el delito de Skimming (delito informático) viene generando inseguridad ciudadana?

Tabla 2: entrevistas por el objetivo general

Entrevistado 01	Entrevistado 02
Considero que, si afecta la inseguridad ciudadana, pues el Skimming, que viene a ser el robo de identidad es uno de los delitos más frecuentes que se cometen en las entidades bancarias y comerciales. El sujeto activo mediante la utilización de engaños, estafas (phishing y malware), manipulan y roban la información los usuarios llegando también a robar las identidades.	Este delito de robo de identidad en transacciones comerciales y bancarias, es uno de los delitos que viene causando preocupación en la seguridad ciudadana, pues es alarmante el nivel de delitos informáticos en especial la suplantación que se viene incrementando dentro de las transacciones.
Entrevistado 03	**Entrevistado 04**
La usurpación de identidad (skimmng) identificado como ciberdelito, que reside en adecuar de los datos de identidad de otra persona, para conseguir un beneficio económico, tomando su identidad. Ningún ciudadano se encuentra seguro de sufrir en algún momento esta	Considero que, si afecta la seguridad ciudadana, debido a que al sustraer la información personal es para ser utilizada para actos ilícitos realizando transacciones comerciales como compras que no han sido autorizadas, retiros de dinero o transferencias,

situación de que te roben tu identidad para realizar transacciones fraudulentas perjudicándote económicamente, por lo tanto, si afecta la seguridad ciudadana.	causando perjuicio económico a cualquier ciudadano.

Entrevistado 05	**Entrevistado 06**
Claro que causa inseguridad ciudadana, los delitos informáticos son ocultos, y difícilmente se detectan, si hasta cuando llega una notificación o revisas tus saldos en las cuentas bancarias; es difícil detectar al sujeto o sujetos que cometen estos ilícitos; por lo tanto, siempre están al asecho de cualquier otra víctima ciudadana.	La seguridad ciudadana si se ve afectada por el skimming, pues el robo de la información personal de una tarjeta de crédito se desarrolla dentro de una transacción totalmente legal.

Entrevistado 07	**Entrevistado 08**
Los delitos informáticos contra el patrimonio si afectan la seguridad ciudadana de la provincia de Chiclayo; la existencia de grupos por bandas criminales dedicada a este ilícito se ha identificado como los tarjeteros del norte, donde según artículos periodísticos también se encuentra conformada por algunos miembros de la PNP.	La situación de la seguridad ciudadana si se ve amenazada por los delitos informáticos que se vienen cometiendo indiscriminadamente contra cualquier ciudadano que tiene una tarjeta de crédito. Siendo común esta situación debido a que hasta los jubilados que están en tercera edad cuentan con una tarjeta de banco.

Ante la pregunta realizada, los entrevistados consideran que, si afecta la inseguridad ciudadana, pues el Skimming, que viene a ser el robo de identidad es uno de los delitos más frecuentes que se cometen en las entidades bancarias y comerciales. El sujeto activo mediante la utilización de engaños, estafas (phishing y malware), manipulan y roban la información los usuarios llegando también a robar las identidades. Ningún ciudadano se encuentra seguro de sufrir en algún momento esta situación de que te roben tu identidad para realizar transacciones fraudulentas perjudicándote económicamente, por lo tanto, si afecta la seguridad ciudadana.

Objetivo Específico a) desarrollar el ilícito informático de Skimming según la Ley 30096 en la legislación penal peruana,

Podría señalarnos en que consiste el delito de Skimming, según la Ley 30096 en la legislación penal peruana

Tabla 3 Entrevistas por el objetivo específico primero

Entrevistado 01	**Entrevistado 02**
Consiste en la suplantación de una persona con la finalidad de causar perjuicio mortal o material.	Es la suplantación de una persona con la finalidad de causar perjuicio o daño a una persona, se encuentra establecido en la ley 30096.
Entrevistado 03	**Entrevistado 04**
Se encuentra como delitos informáticos modernos, señalados en la ley 90096, el cual sanciona la suplantación de personas con el fin de perjudicar a una persona o institución mediante la utilización de tecnologías de la información o de la comunicación.	Es un delito informático donde el sujeto activo suplanta a una persona para cometer un ilícito perjudicando a un tercero. Se encuentra sancionado en la ley 30096 de la legislación peruana.
Entrevistado 05	**Entrevistado 06**
Esta modalidad consiste en copiar la banda magnética de la tarjeta para luego transferir la información confidencial (número y claves) a otra tarjeta en blanco. Una vez realizado este proceso, los delincuentes realizan retiros a través de cajeros	Clonar de tarjetas de crédito: Conducta delictiva cometida “mediante aparatos electrónicos de lectura de bandas magnéticas (skimmer) donde malos empleados de

automáticos o efectúan pagos en dispositivos POS con la tarjeta clonada como si fueran el titular.	restaurantes, gasolineras y otros locales extraen los datos de la tarjeta de crédito. Luego, son copiados a una computadora portátil o personal y, finalmente, copiados a otra tarjeta clonada con los mismos datos personales de la tarjeta original
Entrevistado 07	**Entrevistado 08**
"El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años" En cuanto al sujeto activo, se advierte que este ilícito lo puede cometer cualquier persona y respecto al sujeto pasivo puede ser cometido contra cualquier persona natural o jurídica.	Este tipo penal es mediante clonación o fotos de tarjetas bancarias, para utilizar datos en el fraude informático, y son colocados en los cajeros automáticos o en los agentes, para que la víctima al momento de pasar su tarjeta se almacene dicha información en un dispositivo electrónico.

Las personas entrevistadas describieron cómo los delincuentes copian la información confidencial de las tarjetas de crédito o débito, transferirla a una tarjeta en blanco y luego realizar retiros o pagos con la tarjeta clonada, suplantando la identidad del titular. Esta conducta es penada con una sanción de entre 3 a 5 años de prisión, según la ley. Cualquier persona puede cometer este delito y puede ser cometido contra cualquier persona natural o jurídica.

Objetivo Específico b) describir los aspectos generales y penales de seguridad ciudadana según nuestra norma legal peruana y

¿Podría ilustrarnos que se debe entender por seguridad ciudadana?

Tabla 4: entrevistas por el objetivo específico segundo

Entrevistado 01	**Entrevistado 02**
Viene a ser la acción integrada que despliega el Estado, con la asistencia permanente de la ciudadanía, consignada en aseverar una pacífica convivencia, para erradicar la violencia y la utilización pacífica.	Es la obligación de Estado de implementar mecanismos de protección de la ciudadanía, con la participación y colaboración de esta, y con los mecanismos necesarios
Entrevistado 03	**Entrevistado 04**
La seguridad ciudadana esta referido a la acción integrada, de diversos sectores, intergubernamental y cuya base territorial desarrolla el Estado mediante la colaboración de la ciudadanía con el fin de asegurar respectivamente la protección y pacífica convivencia.	La seguridad ciudadana en el Perú fue creada mediante Ley N°27933, con la finalidad de elaborar y ejecutar políticas públicas de manera coordinada entre todas las instituciones de acuerdo a sus niveles de gobierno, a través de la Conasec y los sus diversos comités distritales, provinciales, regionales.
Entrevistado 05	**Entrevistado 06**
viene a ser el proceso de fortalecer y dar protección al orden democrático, luchando contra la amenaza de violencia en la población lo que permitirá una coexistencia pacífica y pacífica.	La seguridad ciudadana y comunitaria intenta atender indivisas causas permisibles de los ilícitos y de la violencia.

Entrevistado 07	Entrevistado 08
La seguridad ciudadana, se encuentra normado en nuestro país, con la finalidad de comprometer la participación de los diversos sectores de la sociedad, asumiendo un rol protagónico en la asistencia en favor de la comunidad.	La Seguridad Ciudadana, viene a ser el conjunto que relaciona a los organismos públicos y de la sociedad civil, constituido con el fin de favorecer en dar garantía a la tranquilidad y la paz social, reduciendo o neutralizando la criminalidad y delincuencia a nivel nacional.

En su mayoría los entrevistados han conceptualizado que la seguridad ciudadana en el Perú fue creada mediante Ley N°27933, con la finalidad de elaborar y ejecutar políticas públicas de manera coordinada entre todas las instituciones de acuerdo a sus niveles de gobierno, a través de la CONASEC y los sus diversos comités distritales, provinciales, regionales. La seguridad ciudadana esta referido a la acción integrada, de diversos sectores, intergubernamental y cuya base territorial desarrolla el Estado mediante la colaboración de la ciudadanía con el fin de asegurar respectivamente la protección y pacífica convivencia.

Objetivo Específico c) analizar la situación problemática de inseguridad ciudadana producto del inicito de Skimming como modalidad de delito informáticos señalado en la ley 30096.

¿Cuál es su opinión respecto a la inseguridad ciudadana, por delitos informáticos en la provincia de Chiclayo?

Tabla 5: Respuestas por el objetivo específico tercero

Entrevistado 01	**Entrevistado 02**
La llamada ciberdelincuencia viene generando desconfianza de la población en asuntos bancarios, pues los delitos informáticos apuntan a diversos mecanismos para conseguir un provecho económico, vulnerando el derecho de los demás, de esta manera ha vulnerado la seguridad ciudadana.	Los delitos informáticos atacan de manera masiva a personas que cuentan con un margen mínimo de ingreso a la cibernética, desde el momento que realizas un pago con tarjeta, sea crédito, débito o depósitos por bolsillos electrónicos, todos están expuestos a sufrir algún tipo de delito; por lo tanto, la seguridad ciudadana se ve trasgredida ante las distintas formas de delincuencia mediante medios electrónicos.
Entrevistado 03	**Entrevistado 04**
El mal uso de la tecnología que es direccionada a cometer delitos a través de diversas modalidades viene asechando la seguridad ciudadana esto se ve reflejada en las constantes denuncias que se hacen en las comisarías de todas las provincias de nuestro país por delitos de fraude	La seguridad ciudadana si se encuentra asechada e insegura frente al avance tecnológico, pues en cualquier momento y en cualquier transacción que se utilice tu DNI, tarjeta de crédito, o pago en agentes o cajeros electrónicos, cualquier ciudadano puede ser víctima de los delitos cibernéticos

informático, suplantación etc que son los más frecuentes.	
Entrevistado 05	**Entrevistado 06**
La ciberdelincuencia se viene sofisticando cada día más en gran medida de acuerdo a los avances tecnológico. Esta situación de amenaza informática viene creando un significativo impacto dentro de la sociedad que forma parte del sistema financiero, mediante estafas digitales; esta situación crea mucha inseguridad en la ciudadanía.	La seguridad ciudadana si se afecta con cualquier delito que tiene incidencia y se cometa a varios ciudadanos, el delito de skimming, no se detecta de manera automática, pues las amenazas informáticas se cometen desde cualquier lugar, pero afectan económicamente al propietario de la tarjeta.
Entrevistado 07	**Entrevistado 08**
La delincuencia, mediante medios tecnológicos aprovecha para cometer diversos delitos como es el caso de la suplantación de identidad en las tarjetas de crédito o débito, que cualquier ciudadano usa de manera legal en una transacción, esta suplantación de identidad, viene a ser un fenómeno delincuencial que toma fuerza ante la vulnerabilidad y confianza en la población.	La suplantación de identidad (skimming), es un procedimiento que repercute en el daño económico, daño moral sobre la víctima en diversos casos el perjuicio se manifiesta a largo plazo, también existen casos donde se detecta de manera inmediata mediante mecanismos de prevención, por lo tanto, si afecta la seguridad ciudadana.

¿Considera que los delitos informáticos que se han incrementado en la provincia de Chiclayo?

Tabla 6: entrevistas por el objetivo específico tercero

Entrevistado 01	**Entrevistado 02**
Si, se han incrementado, siendo las fuentes de información los cuerpos especiales de delitos informáticos de la PNP, quienes dan a conocer el robo de datos personales y fondos económicos que son denunciados en las comisarías del sector.	En la Divincri Chiclayo, se vienen registrando un promedio de 185 denuncias de delitos informáticos de este tipo (skimming); estas mafias se esconden en plataformas tecnológicas utilizando la ingeniería social utilizando personas con necesidades económicas.
Entrevistado 03	**Entrevistado 04**
Si existe un incremento de delitos informáticos, en diversas modalidades, siendo el sector comercio donde se aprecia la suplantación de tarjetas, robo de identidades, que difícilmente capturan a los sujetos.	Si se ha incrementado, habiendo identificado bandas criminales como los tarjeteros del norte, quienes planifican y ejecutan sus robos en los agentes bancarios del centro e Chiclayo.
Entrevistado 05	**Entrevistado 06**
La policía de investigación criminal divincri, reportó diversas bandas criminales dedicadas a la clonación de tarjetas y robo de identidad de estas, siendo el Banco de la nación y los agentes y cajeros automáticos de la ciudad de Chiclayo	Por supuesto que existe un incremento, la delincuencia va en aumento en diversas modalidades siendo los delitos informáticos quienes vienen incrementándose en diversas modalidades.

Entrevistado 07	Entrevistado 08
Existe un considerable incremento en lo que, de los últimos años, las denuncias en las comisarías del sector así lo demuestran, Ha presentado una tendencia creciente, siendo el valor más alto es en el año 2022 (tasa de 0.74%).	Los robos informáticos mediante la modalidad de transferencias bancarias y por intermedio de aplicativos digitales, se han incrementado en la provincia de Chiclayo.

Los entrevistados de manera categórica, han señalado que han incrementado, siendo las fuentes de información los cuerpos especiales de delitos informáticos de la PNP, quienes dan a conocer el robo de datos personales y fondos económicos que son denunciados en las comisarías del sector. Siendo la Divincri PNP Chiclayo, donde se vienen registrando un promedio de 185 denuncias de delitos informáticos de este tipo (skimming); estas mafias se esconden en plataformas tecnológicas utilizando la ingeniería social utilizando personas con necesidades económicas.

Triangulacion de las categorías y subcategorias.

Tabla 7: Categoría 01.- El Skimming como modalidad de delito informáticos en la ley 30096

Objetivo general	Normativa	Doctrina	Jurisprudencia	Opinion de los entrevistados	Opinion del entrevistador	conclusion
Determinar la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo en el año 2022	Ley 30096 ley de delitos informáticos .	Fernández (2020), esta relacionada con la ciberdelincuencia o criminalidad informática, en sentido amplio, como actividades delictivas relacionadas al empleo de tecnologías de la información y de la comunicación.	Exp.N.° 01189-2019-PHC/TC delitos de fraude informático y falsificación de firma en documento privado.	Los entrevistados señalan que el delito de el Skimming, es el robo de identidad que se comete frecuentemente en las entidades bancarias y comerciales.	De acuerdo a lo que señala la doctrina el Eskimming, forma parte de los delitos informaticos señalados en la ley 30096, considerado dentro de la diberdelincuencia, esta posicion se corrobora con la opnión de los entrevistados queienes además señalan que esun delito frecuente en nuestra soceidad. Debido a que no existen estrategias de seguiridad ciudadana que protegan estas zonas.	Nuestra socedad de la provincia de Chuiclayo, se encuentra amenazada pot organizaciones criminales que lleban a cabo la ciberdelinuencia en sus diversas modalidades, siendo una de las más incidenctes el Skiming que la usurpación de indetidad, existen actualmente escasa jurisprudenica nacional respeto a estos ilicitos.

Categoría 01.- ***El Skimming como modalidad de delito informáticos en la ley 30096***

Tabla 8: Primer objetivo Específico

Objetivo especifico	Normativa	Doctrina	Jurisprudencia	Opinion de los entrevistados	Opinion del entrevistador	conclusion
Desarrollar el ilícito informático de Skimming según la Ley 30096 en la legislación penal peruana,	Ley 30096 ley de delitos informáticos. Articulo 9º Suplantación de identidad mediante tecnologías digitales.	Espinoza, (2022) Señala que El “skimming” consiste en la extracción de datos de una tarjeta de créditos o débitos en determinado centro de ventas, mediante unos dispositivos electrónico portátil llamado “skimmer”.	Exp.N.° 01189-2019-PHC/TC delitos de fraude informático y falsificación de firma en documento privado.	Los entrevistados señalan que el delito se desarrolla mediante el clonado de la banda magnética de la tarjeta para luego transferir la información confidencial (número y claves) a otra tarjeta en blanco. Una vez realizado este proceso, los delincuentes realizan retiros a través de cajeros automáticos o efectúan pagos en dispositivos P.O.S con la tarjeta clonada como si fueran el titular.	Con elpresente objetivo se pretende obtener los aspectos generales del delito de Skimming el cual se encuentra establecido en una ley especial que es la 30096, el nivel de conocimento que expresan los entrevistados es mayoritaria al calificarlo como el acto de clonar los datos de una banda magnética de la tarjeta de debito o credito y luego transferir dicha información a otra tarjeta en blanco.	El Skimming es el delito que consiste en la extracción de datos confidenciales de una tarjeta de credito o debito para trasladarlos a otra tarjeta con fines delincuenciales, esta considerado como delito especial según el articulo 9 de la ley 30096, este ilicito ha sido identificado por los entreviostados como incidente en nuestra provincia.

Categoría dos: Niveles de inseguridad ciudadana en la provincia de Chiclayo Región Lambayeque.

Tabla 9: Segundo objetivo Específico

Objetivo especifico	Normativa	Doctrina	Jurisprudencia	Opinion de los entrevistados	Opinion del entrevistador	conclusion
Describir los aspectos generales y penales de seguridad ciudadana según nuestra norma legal peruana.	Ley N°27933, de Seguridad ciudadana.	Vizcarra (2023) la seguridad ciudadana se derine como aquella situación social caracterizada en un clima de paz, de armonía, de convivencia entre los ciudadanos, facilitabndo el libre y pacífico ejercicio de los derechos individuales, políticos y sociales	Decreto Legislativo N° 1351 Modifica normas de seguridad ciudadana	Los entrevistados señalan que Ley N°27933, de seguidad ciudadana debe cumplir el fin por la cual fue reada como es la elaboración y ejecución de políticas públicas coordinadas entre todas las instituciones acorde a niveles de gobierno distritales, provinciales, regionales.	El opbjetivo esta orientado a ver las consecuencias que genera el ilicito de skimming en el contexto de seguridad ciudadana, la misma que se ve vulnerada por grupos que cometen ciberdelincuencia en centros cmerciales, agentes bancarios, etc, mediante dispositivos electrónicos.	La seguridad ciudadana se encuentra regulada en la ley 27933, La seguridad ciudadana se refiere a diversas acciones integradas, por distintos y diversos sectores, intergubernamentales de nuestro país, eso se realiza con la colaboración de la ciudadanía para proteger y sostener una convivnencia pacífica en sociedad.

Categoría dos: Niveles de inseguridad ciudadana en la provincia de Chiclayo Región Lambayeque.

Tabla 10: Tercer objetivo Específico

Objetivo especifico	Normativa	Doctrina	Jurisprudencia	Opinion de los entrevistados	Opinion del entrevistador	conclusion
Analizar la situación problemática de inseguridad ciudadana producto del inicito de Skimming como modalidad de delito informáticos señalado en la ley 30096.	Ley N°27933, de Seguridad ciudadana. Ley N°27933, de Seguridad ciudadana.	Rivera (2022) Respecto a la problemáticaque causa el ilícirto de skimming, la consdera como acciones de oportunidad donde el ciberdelincuente saca provecho de la situación para su comisión, provocando grandes pérdidas económicas a los afectados y beneficios a sus autores. Presentan gran facilidad para comerter dichos actos en un plazo mínimo y sin la necesidad de la presencia física de sus actores.	Decreto Legislativo N° 1351 Modifica normas de seguridad ciudadana	Los entrevistados señalan que estos delitos actualmente se han incrementado, esa nformacion se ha obtenido en los cuerpos especiales de delitos informáticos de la PNP, (divincri) quienes dan a conocer el robo de datos personales y fondos económicos que son denunciados en las comisarías del sector. Siendo la Divincri PNP Chiclayo, donde se vienen registrando un promedio de 185 denuncias de delitos informáticos de este tipo (skimming).	El opbjetivo esta orientado al análisis de la situación actual respecto a la afectación que viene causando el delito del skimming en la la seguridad ciudadana de la provincia de Chiclayo, la misma que es considerada por los entrevistados como existen muchas denuncias en divincri, (185 denucnias promedio) las cuales han causado perjuicio económico despues de haberse clonado sus datos personales en las tarjetas de crédito y debito.	Efectivamente la inseguridad ciudadana especialmente en las zonas comerciales y agentes financieros se ven afectados por grupos criminales que se dedican a la ciberdelincuencia medinte el delito de skimming (suplantando la identidad, medinate el robo de datos personales que existen en las tarjetas). Además existe en la divincri, registradas diversas bandas criminales.

4.2.- Discusión de resultados

De acuerdo al objetivo general es: determinar la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo en el año 2022.

¿Usted considera que el delito de Skimming (delito informático) viene generando inseguridad ciudadana?

Ante la pregunta realizada, los entrevistados consideran que, si afecta la inseguridad ciudadana, pues el Skimming, que viene a ser el robo de identidad es uno de los delitos más frecuentes que se cometen en las entidades bancarias y comerciales. El sujeto activo mediante la utilización de engaños, estafas (phishing y malware), manipulan y roban la información los usuarios llegando también a robar las identidades. Ningún ciudadano se encuentra seguro de sufrir en algún momento esta situación de que te roben tu identidad para realizar transacciones fraudulentas perjudicándote económicamente, por lo tanto, si afecta la seguridad ciudadana.

Esta posición que adoptan los entrevistados, tiene coincidencia con el objetivo en análisis pues de manera general los entrevistados coinciden con nuestra posición indicando que, si vienen generando un nivel de inseguridad ciudadana, por lo que se hace necesario que los operadores de justicia planifiquen y ejecuten medidas de política criminal.

Con los antecedentes

Según Padilla (2022), en su estudio sobre "Inseguridad ciudadana y delitos de mayor connotación social: formas y extensiones del temor a la delincuencia en Chile", se analiza la percepción de inseguridad ciudadana en Chile, especialmente en relación con delitos que generan gran impacto social. Se concluye que no se debe minimizar la importancia de los delitos contra la propiedad, ya que, aunque su magnitud sea menor que otros tipos de delitos, estos ilícitos representan una violación de espacios que antes eran seguros y confortables para las personas, y además implican significativas pérdidas económicas.

La posición del autor tiene coincidencia con el presente objetivo que analiza la si la incidencia de ilícitos informáticos viene generando inseguridad ciudadana en la provincia de Chiclayo, pues señala que en Chile los delitos informáticos en Chile van de manera escalonada, siendo el Estado quien asume más responsabilidad en la protección, pues estos delitos son considerando informáticos cometidos contra ciudadanos comunes y corrientes son considerados como de primera subdimensión, así la seguridad ciudadana debe ser favorecida mediante campañas urgentes requiriendo el aumento de su cobertura y difusión, es un mecanismo disuasivo al usuario para adoptar medidas de cuidado y siguiendo el protocolo establecido.

Doctrina

Según Padilla (2022), en su estudio sobre "Inseguridad ciudadana y delitos de mayor connotación social: formas y extensiones del temor a la delincuencia en Chile", se analiza la percepción de inseguridad ciudadana en Chile, especialmente en relación con delitos que generan gran impacto social. Se concluye que no se debe minimizar la importancia de los delitos contra la propiedad, ya que aunque su magnitud sea menor que otros tipos de delitos, estos ilícitos representan una violación de espacios que antes eran seguros y confortables para las personas, y además implican significativas pérdidas económicas.

La definición expuesta, permite entender que todos los ciudadanos mayores de edad, que es común que en estos tiempos la tecnología nos obliga a contar con una tarjeta sea de crédito o débito, estamos expuestos a un tipo de fraude informático, en cualquier momento y lugar donde nos encontremos haciendo una transacción comercial o financiera; por lo tanto, este concepto si tiene relación con el objetivo en análisis, entendiendo que la seguridad ciudadana si se encuentra amenazada por este tipo de ilícito.

Objetivos específicos a) desarrollar el ilícito informático de Skimming según la Ley 30096 en la legislación penal peruana.

Desde las entrevistas

Se plantearon la pregunta ¿Podría señalarnos en que consiste el delito de Skimming, según la Ley 30096 en la legislación penal peruana? Siendo las en su mayoría las respuestas de los entrevistados, que Esta modalidad implica la clonación de tarjetas, donde se copia la información confidencial de la banda magnética de una tarjeta original y se transfiere a una tarjeta en blanco. Posteriormente, los delincuentes utilizan la tarjeta clonada para realizar retiros de efectivo en cajeros automáticos o efectuar pagos en dispositivos de punto de venta (P.O.S.) como si fueran el legítimo titular de la tarjeta; la penalidad por suplantar la identidad de una persona o entidad a través de tecnologías de la información o comunicación, causando daño material o moral, es una pena de prisión de entre 3 a 5 años. Cualquier individuo puede cometer este delito y puede ser cometido en contra de cualquier persona o entidad, ya sea natural o jurídica.

Desde los antecedentes

La investigación de Aldecoa (2020), analiza la suplantación de identidad y los medios informáticos en el sector financiero año 2019 el Lima, con el objetivo en determinar las formas en que los medios informáticos favorecen la comisión del delito de suplantación de identidad donde concluye que el skimmng, es un mecanismo tecnológico que se aplica para lograr la obtención de datos personales directos de la víctima mediante herramientas tecnológicas de un usuario del banco, favoreciendo así la perpetración del ilícito de suplantación de identidad.

La investigación se condice con nuestro objetivo en desarrollo, al describir aspectos de la suplantación de identidad, el autor señala que se necesita una actualización inmediata de la norma Ley N° 30096, Ley de Delitos Informáticos, señala que en la actualidad se han incrementado los ilícitos informáticos en diversas modalidades contempladas en esta norma, pues la naturaleza de esta

ley, aparte del incremento del uso de las tecnologías de la información y la comunicación ameritan una modificatoria y regulación exhaustiva.

Desde la doctrina

La doctrina de Según Delgado (2021), anteriormente se utilizaba el término "delitos informáticos" para describir aquellos delitos cometidos mediante o en contra de sistemas informáticos. Sin embargo, en la actualidad, estos delitos han evolucionado y ahora pueden ser cometidos a través de diversas plataformas, incluyendo páginas web, redes sociales, dispositivos electrónicos de información y comunicación, lo que genera una creciente preocupación en el ámbito del sistema penal.

Posición que se condice con nuestro objetivo, pues estos delitos que, sin difícilmente de detectar al sujeto activo, son los que vienen ocurriendo de manera creciente en nuestra sociedad, generalmente son los mega plazas, o financieras los lugares que son más frecuentes para cometer este ilícito.

Objetivos específicos b) describir los aspectos generales y penales de seguridad ciudadana según nuestra norma legal peruana

Desde las entrevistas

Se plantearon la siguiente interrogante ¿Podría ilustrarnos que se debe entender por seguridad ciudadana?, en su mayoría los entrevistados han conceptualizado que la seguridad ciudadana en el Perú fue creada mediante Ley N°27933, con la finalidad de elaborar y ejecutar políticas públicas de manera coordinada entre todas las instituciones de acuerdo a sus niveles de gobierno, a través de la CONASEC y los sus diversos comités distritales, provinciales, regionales. La seguridad ciudadana esta referido a la acción integrada, de diversos sectores, intergubernamental y cuya base territorial desarrolla el Estado mediante la colaboración de la ciudadanía con el fin de asegurar respectivamente la protección y pacífica convivencia.

Los entrevistados se fundamentan desde el punto de vista legal en definir la seguridad ciudadana, señalando la norma de creación y los comités de organización, además la funciones específicas y coordinación con sectores de la sociedad y su respectiva participación.

Desde los antecedentes

Se cita la investigación de Villanueva (2023) ley de los delitos informáticos Nº30096 y su influencia en la población de Chiclayo, en tiempos de pandemia covid-19", con el fin de determinar la forma en que la Ley de delitos informáticos N°30096, influye en la población de Chiclayo, concluyendo que durante ese periodo si existió una correlación positiva, indicando que los delitos informáticos de manera significativa trasgreden el factor económico e integridad personal de sus víctimas.

Esta posición es una muestra de que, desde los tiempos de pandemia, se viene incrementando los ilícitos informáticos en los pobladores de Chiclayo, lo que ha generado una afectación moral, integridad física e integridad psíquica, representando el 36.8%, de delitos denunciados y el autor hace la

recomendación de denunciar estos actos que cuentan con una norma especial sancionadora que es la Ley 30096.

Desde la doctrina

Según Huerta (2019) El concepto de seguridad ciudadana abarca las dimensiones que lo integran, definiéndolo como aquella situación social que se caracteriza por un clima de paz, de armonía, de convivencia entre los ciudadanos, que permite y facilita el libre y pacífico ejercicio de los derechos individuales, políticos y sociales, así como el normal funcionamiento de las instituciones públicas y privadas.

Este concepto tiene relación con el objetivo en análisis al señalar que su característica es que se crea para una mejor convivencia con un clima de paz social; la mima que es vulnerada por actos delictivos como son los actos criminales y diversos delitos como en este caso se analiza los delitos informáticos.

Objetivos específicos c) analizar la situación problemática de inseguridad ciudadana producto del inicito de Skimming como modalidad de delito informáticos señalado en la ley 30096.

Desde las entrevistas

Se plantearon las siguientes preguntas ¿Cuál es su opinión respecto a la inseguridad ciudadana, por delitos informáticos en la provincia de Chiclayo? Y la siguiente pregunta fue ¿Considera que los delitos informáticos que se han incrementado en la provincia de Chiclayo? Los entrevistados de manera categórica, han señalado que han incrementado, siendo las fuentes de información los cuerpos especiales de delitos informáticos de la PNP, quienes dan a conocer el robo de datos personales y fondos económicos que son denunciados en las comisarías del sector. Siendo la Divincri PNP Chiclayo, donde se vienen registrando un promedio de 185 denuncias de delitos informáticos de este tipo (skimming); estas mafias se esconden en plataformas tecnológicas utilizando la ingeniería social utilizando personas con necesidades económicas.

Los entrevistados refuerzan nuestra preocupación del incremento de delitos informáticos como es el skimming, afirmando que existe un considerable incremento de actos ilícitos, que deben ser tomados en cuenta por parte de los operadores de justicia.

Desde los antecedentes

La investigación realizada por Bernal en 2022 tuvo como objetivo identificar las causas que afectan la eficacia del trabajo de los especialistas en administrar justicia (policías, fiscales y jueces) en la investigación y juzgamiento de ciberdelitos y otros ilícitos relacionados. Los resultados mostraron una relación significativa entre el patrullaje cibernético y el desarrollo de la seguridad ciudadana en una entidad policial pública de Chiclayo en 2022, lo que sugiere que el patrullaje cibernético es un factor importante para mejorar la seguridad ciudadana en el contexto de la lucha contra los ciberdelitos.

De esta investigación entendemos que el autor ha logrado demostrar el vínculo significativo que se presenta entre la planificación de seguridad con la evolución

de la seguridad ciudadana en una institución estatal de la Policía que labora en Chiclayo, sugiriendo que la junta vecinal tiene que realizar una labor de forma conjunta con la comisaria con la finalidad disminuir los ilícitos cibernéticos.

Desde la doctrina

Según Vizcarra (2023) La seguridad ciudadana abarca un conjunto de aspectos que garantizan el bienestar y protección de las personas y la sociedad, incluyendo la seguridad jurídica, social, ambiental, y económica, así como el respeto a los derechos humanos y la lucha contra la pobreza. Cuando las personas pueden desarrollar sus actividades sin miedo a sufrir daños o menoscabos en cualquier ámbito, y pueden ejercer sus derechos y libertades de manera responsable y libre, se puede afirmar que se ha logrado la seguridad ciudadana.

De acuerdo a esta doctrina para hacer frente a los ilícitos que se arremeten en la sociedad Chiclayana, es necesario que la ley y lo parámetros establecidos en diferentes documentos, se ejecuten de manera conjunta por todas la autoridades o instituciones implicadas en ella, siendo un actividad constante para poder hacer frente a la delincuencia, en este caso a la delincuencia cibernética, en específico al delito de skimming, que es uno de los más frecuentes que se viene cometiendo en la ciudad de Chiclayo.

CONCLUSIONES

Primera: La usurpación de identidad (skimmng) identificada en el sistema penal según la ley 30096, es un ciberdelito, que se ejecuta robando los datos de identidad de otra persona mediante sistema electrónico en las tarjetas de crédito o débito, con el fin de un beneficio económico. Ningún ciudadano se encuentra seguro de sufrir en algún momento esta situación de que te roben tu identidad para realizar transacciones fraudulentas perjudicándote económicamente, por lo tanto, si afecta la seguridad ciudadana.

Segunda: Son delitos informáticos modernos, señalados en la ley 90096, el cual sanciona la suplantación de personas con el fin de perjudicar a una persona o institución mediante la utilización de tecnologías de la información o de la comunicación, mediante tarjetas de crédito: Se comete un delito cuando se utiliza un dispositivo electrónico llamado skimmer para copiar la información de una tarjeta de crédito o débito y luego se transfiere a una computadora portátil o personal, finalmente se clona la tarjeta con los mismos datos personales de la tarjeta original. Esto es considerado suplantación de identidad y está penado con una pena de prisión de entre 3 a 5 años si se causa algún perjuicio material o moral. Cualquier persona puede cometer este delito y puede ser cometido en contra de cualquier persona natural o jurídica.

Tercera: La seguridad ciudadana en el Perú fue creada mediante Ley N°27933, con la finalidad de elaborar y ejecutar políticas públicas de manera coordinada entre todas las instituciones de acuerdo a sus niveles de gobierno, a través de la CONASEC y los sus diversos comités distritales, provinciales, regionales. La Seguridad Ciudadana, viene a ser el conjunto que relaciona a los organismos públicos y de la sociedad civil, constituido con el fin de favorecer en dar garantía a la tranquilidad y la paz social, reduciendo o neutralizando la criminalidad y delincuencia a nivel nacional.

Cuarta: De acuerdo a los entrevistados se considera que, si existe un incremento de delitos informáticos, en diversas modalidades, siendo el sector comercio donde se aprecia la suplantación de tarjetas, robo de identidades, que difícilmente capturan a los sujetos. La policía de investigación criminal divincri, reportó diversas bandas criminales dedicadas a la clonación de tarjetas y robo de identidad de estas, siendo el Banco de la nación y los agentes y cajeros automáticos de la ciudad de Chiclayo.

RECOMENDACIONES

- Al haberse identificado el modus operandi del delito de usurpación de identidad (skimmng) en el sistema penal según la ley 30096, los operadores de justicia mediante un plenario, o jurisprudencia debe de aplicar una política criminal con sanciones drásticas, pues la sanción actual establece penas menores a cinco años, lo que hace permisible que estos sujetos continúen cometiendo diversas modalidades de ilícitos cibernéticos.

- A las autoridades correspondientes (parlamentarias), y los operadores de justicia deben de legislar los delitos informáticos de manera minuciosa, con el fin de salvaguardar el derecho a la intimidad de los ciudadanos. Al observar actualmente una proliferación constante de modalidades, hackeos, suplantaciones y otras que comprometen la seguridad de la información de los individuos. Además, se debe implementar programas destinados a comprender la naturaleza de estos actos delictivos.

- El Estado mediante las autoridades correspondientes deben de efectivar lo que establece la norma (Ley N°27933) y los acuerdos concordantes que se refieren al fortalecimiento de la seguridad ciudadana, pues en escrito está la elaboración y ejecución de políticas públicas coordinada entre todas las instituciones acorde a niveles de gobierno mediante la CONASEC; sin embargo, existe en la actualidad descoordinación entre las autoridades, no existe logística, personal, etc, que permitan fortalecer un efectivo tratamiento contra la delincuencia cibernética.

- Se debe fortalecer la logística de la Policía Nacional, ampliando personal para la detección de sistemas piratas, y se pueda hacer identificación inmediata de aquellos sujetos que vienen cometiendo ilícitos contra la ciudadanía de Chiclayo, además de difundir en diversas entidades y centros comerciales diversas medidas de precaución para no ser víctimas de estos delitos informáticos como es la suplantación de identidad.

Bibliografía

Aldecoa, J. M. (2020). *El delito de suplantación de identidad y los medios informáticos, en el sector financiero de Lima 2019.* Obtenido de https://acortar.link/q9rvsz

Arce, J. (2020). *Politica criminal y delitos informáticos.* Buenos Aires: Huammurabi.

Carrera, Y. M. (2023). *Fundamentos Juridicos para incorporar el Phising como agravante en el articulo 11 de la Ley 30096-Ley de los delitos informaticos en el Peru.* Obtenido de https://acortar.link/Rk9vKZ

Castillo, E., & Vásquez, M. L. (2003). *El rigor metodológico en la investigación cualitativa.* Obtenido de https://colombiamedica.univalle.edu.co/index.php/comedica/article/view/269#:~:text=La%20credibilidad%20se%20logra%20cuando,contacto%20con%20el%20fen%C3%B3meno%20investigado.

CEPA, C. e. (2022). *Panorama del derecho informático en América Latina y el Caribe .* Mexico: ECLAC.

Cumpa, C. Y. (2021). *Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude inforamtico.* Obtenido de https://acortar.link/KHgy6Z

Defensoría del Pueblo. (2024). *La Ciberdelincuencia En El Perú: E.* 2024: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf.

Durán, M. E. (2022). *El saber pedagógico de los profesores de la Universidad de Los Andes Táchira y sus implicaciones en la enseñanza.* Obtenido de EL CARÁCTER CIENTÍFICO DE LA INVESTIGACIÓN: https://www.tdx.cat/bitstream/handle/10803/8922/10CapituloXElcaracterCientificodelainvestigaciontfc.pdf?sequence=3#:~:text=El%20rigor%20ci

ent%C3%ADfico%20en%20torno,concordancia%20con%20el%20proceso%20seguido

Elías, R. (2020). *Luces y sombras en la lucha contra la delincuencia informática en el Perú.* Lima: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf.

Espinoza, C. V. (2022). *"Delitos informáticos y nuevas Modalidades delictivas".* Instituto Pacífico. doi:.

Espinoza, C. V. (2022). *Delitos informáticos y nuevas modalidaes delictivas.* Lima: Instituto Pacifico.

Estrada, R. J. (2015). *Democracia, Estado y seguridad ciudadana.* Lima: Flacso.

Fernandez, B. (2020). *Ciberdelito.* Madrid: Experiencia.

Gonzales, M. (2022). *La entrevista cualitativa como técnica de investigación en el estudio de las organizaciones.* https://www.researchgate.net/.

Guevara, G. (2020). *Metodologías de investigación educativa.* 0: RECIMUND.

Hernández, S. R. (2021). *Validación de un instrumento que mide el perfil actitudinal de los docentes y el desarrollo de competencias universitarias y transversales*. Obtenido de https://www.scielo.org.mx/pdf/ride/v12n23/2007-7467-ride-12-23-e011.pdf

Inga, M. (2020). *Metodos de recoleccion de datos para una investigación .* Editorial Prentice. doi:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://fgsalazar.net/LANDIVAR/ING-PRIMERO/boletin03/URL_03_BAS01.pdf

Martinez, J. (2023). *Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo.* Dialnet.

Miguélez, M. M. (2021). *Validez y confiabilidad en la metodología cualitativa*. Obtenido de https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1011-22512006000200002

Molinos, C. A. (2020). *El Fraude Informático y Telemático: Perspectiva Penal Valladolid,.* Valladolid: https://uvadoc.uva.es/bitstream/handle/10324/46997/TFG-D_01089.pdf?sequence=1&isAllowed=y.

Narvaez, M. (2022). *¿Qué es la validez y confiabilidad en la investigación?* QuestionPro. doi:https://www.questionpro.com/blog/es/que-es-la-validez-y-confiabilidad-en-la-investigacion/

Padilla, G. &. (2022). Inseguridad ciudadana y delitos de mayor connotacion social: formas y extensiones del temor a la delincuencia en Chile. *Cuaderno Urbano*, 22. Obtenido de https://acortar.link/pQjPXQ

Palacios, V. J. (2020). *Metodología de la Investigación Juridica.* Lima: Grijley.

Piña, L. (2023). *El enfoque cualitativo: Una alternativa compleja dentro del mundo de la investigación.* Revista Arbitrada Interdisciplinaria Koinonía.

Quintero, O. (2020). *Problemas de persiguibilidad de los ciberdelitos.* Buenods Aires: Hammurabi.

Rivera, V. D. (2022). *Los delitos informáticos y su incidencia en la gestión de las instituciones del Estado del distrito de huánuco, 2017.* Huanuco: UNHV .

Rodriguez, J. (2022). *Participantes o colaboradores informantes, criterio de saturación de información en estudios cualitativos.* Guanajuato: https://blogs.ugto.mx/rea/clase-digital-8-participantes-o-colaboradores-informantes-criterio-de-saturacion-de-informacion-en-estudios-cualitativos/.

Sierra, L. C. (2022). *Percepción de Inseguridad de los Ciudadanos de Bucaramanga y Floridablanca.* Obtenido de https://acortar.link/XZitoI

Torres, X. (2021). *¿Qué es el grooming? Regulación en el Perú y análisis. Artículo publicado.* Parthenon, el portal web de actualidad jurídica de la Asociación Civil.

Vásquez, F. M. (2020). *Factores de Riesgo de los Cibercrímenes Sociales y su Influencia en los Jóvenes de la.* Obtenido de https://acortar.link/FLw1xK

Vizcarra, C. (2023). *Seguridad ciudadana en el Perú.* Lima: PUCP.

PRESENTACIÓN DE INSTRUCCIONES:

A continuación, a usted le presento el cuestionario: ***"El Skimming como modalidad de delito informáticos en la ley 30096, y los niveles de inseguridad ciudadana en la provincia de Chiclayo Región Lambayeque"*** Elaborado por la Bachiller: Cesar Ivan Espinoza Bravo, de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión
	3. Acuerdo (moderado nivel).	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observacinnes que considere pertinente.

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Mg. Mónica Y. Mejía Cusma
DERECHO / GESTIÓN PÚB
ICAL

Mag.....

Anexo 02: Ficha de entrevista

FORMATO DE LA ENTREVISTA

I. Datos generales:

Nombre: _____ Entidad donde labora: _____

Colegiatura: _____ Cargo : _____

Condición laboral: Nombrado ( ) Contratado ( ) Independiente ( )

II. INSTRUCCIONES:

Estimado (a) operador de a justicia, en el presente cuestionario respecto a la investigación: "El Skimming como modalidad de delito informáticos en la ley 30096, y los niveles de inseguridad ciudadana en la provincia de Chiclayo Región Lambayeque". Le solicitamos respuestas objetivas, a cada una de las preguntas formuladas, lo que nos permitirá el desarrollo de nuestra investigación:

De acuerdo al objetivo general:

Determinar la incidencia del Skimming como modalidad de delito informáticos señalado en la ley 30096, que genera inseguridad ciudadana en la provincia de Chiclayo en el año 2022.

De acuerdo a los objetivos específicos:

Objetivo específico uno: desarrollar el ilícito informático de Skimming según la Ley 30096 en la legislación penal peruana

Podría señalarnos en que consiste el delito de Skimming según la Ley 30096

_____

_____

_____

Objetivo específico dos: Describir los aspectos generales y penales de seguridad ciudadana según nuestra norma legal peruana.

Podría ilustrarnos que se debe entender por seguridad ciudadana:

_____

_____

_____

Considera que el nivel de inseguridad ciudadana, se ve afectado por los delitos informáticos, de manera específica el Skimming según la Ley 30096.

Objetivo específico tres: Analizar la situación problemática de inseguridad ciudadana producto del inicio de Skimming como modalidad de delito informáticos señalado en la ley 30096.

Cual es su opinión respecto a la inseguridad ciudadana, por delitos informáticos en la provincia de Chiclayo.

Considera que los delitos informáticos se han incrementado en la provincia de Chiclayo:

Mg. Mónica Y. Mejía Cusma
DERECHO - GESTIÓN PÚBLICA

Mg.
Firma Valoración

Anexo 03: Matriz de categorización

Categoría de estudio	Definición conceptual	Subcategoría	Instrumento
Categoría uno: El Skimming como modalidad de delito informáticos en la ley 30096,	Consiste en la extracción de datos de una tarjeta de créditos o débitos en determinado centro de ventas, mediante unos dispositivos electrónico portátil llamado “skimmer” que es una lectora de banda magnética de las tarjetas plastificadas, son incorporados y aprovechando la tecnología de cajero automático. (Espinoza C. V., 2022)	Definición del Skimming Orígenes del Skimming Los tipos de Skimming Clonación de tarjetas Antecedentes Consecuencias Delincuencia cibernética Sujetos Tipos	Entrevistas Análisis documental
Categoría dos: Seguridad ciudadana	Es un concepto complejo, eminentemente sociopolítico y que se puede definir como aquella situación social que se caracteriza por un clima de paz, de armonía, de convivencia entre los ciudadanos, que permite y facilita el libre y pacífico ejercicio de los derechos individuales, políticos y sociales, así como el normal funcionamiento de las instituciones públicas y privadas (Estrada, 2015)	Realidad Seguridad Normas y participación Sistema de protección legal. Características	Entrevistas Análisis documental