UNIVERSIDAD ESTATAL

PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y SALUD

CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

TÍTULO:

ESTUDIO COMPARADO A LAS NORMAS DE ECUADOR, VENEZUELA Y PERÚ CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS POR ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS

AUTOR:

VILLACRESES SUAREZ KEVIN GEOVANNY

TUTOR: DC. CRISTOBAL MACHUCA REYES, MGT.

LA LIBERTAD – ECUADOR

2023

UNIVERSIDAD ESTATAL

PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y SALUD

CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

TÍTULO:

ESTUDIO COMPARADO A LAS NORMAS DE ECUADOR, VENEZUELA Y PERÚ CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS POR ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS

AUTOR:

VILLACRESES SUAREZ KEVIN GEOVANNY

TUTOR: DC. CRISTOBAL MACHUCA REYES, MGT.

LA LIBERTAD – ECUADOR

2023

La Libertad, de 22 de noviembre del 2023

APROBACIÓN DE TUTOR

En mi calidad de Profesor Turo del Trabajo de Integración Curricular de título: "**ESTUDIO COMPARADO A LAS NORMAS DE ECUADOR, VENEZUELA Y PERÚ CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS POR ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOSESTUDIO COMPARADO ALAS NORMAS DE ECUADOR, VENEZUELA Y PERÚ CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS POR ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS"**, correspondiente al estudiante **KEVIN GEOVANNY VILLACRESES SUAREZ,** de la Carrera de Derecho, de la Universidad Estatal Península de Santa Elena, declaro que luego de haber orientado científica y metodológicamente su desarrollo el referido proyecto de investigación se encuentra concluido en todas sus partes cumpliendo así con el proceso de acompañamiento determinado en la normativa interna, recomendando se inicien los proceso de evaluación que corresponden.

Atentamente

CRISTOBAL HOMERO MACHUCA REYES

Firmado digitalmente por CRISTOBAL HOMERO MACHUCA REYES

Dr. Cristóbal Machuca Reyes.

TUTOR

VALIDACION GRAMATICAL Y ORTOGRAFICA

Certificación de Gramatólogo

Lic. ALEXI JAVIER HERRERA REYES
Magíster En Diseño Y Evaluación De Modelos Educativos

La Libertad, noviembre 21 del 2023.

Certifica:

Que después de revisar el contenido del trabajo de integración curricular en opción al título de **ABOGADO** de: **VILLACRESES SUAREZ KEVIN GEOVANNY,** cuyo tema es: **"ESTUDIO COMPARADO A LAS NORMAS DE ECUADOR, VENEZUELA Y PERÚ CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS POR ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS",** me permito declarar que el trabajo investigativo se encuentra idóneo y puede ser expuesto ante el jurado respectivo para la defensa del tema en mención.

Es todo cuanto puedo manifestar en honor a la verdad.

Lic. Alexi Herrera R. MSc.
Docente de Español A: Literatura
Cel: 0962989420
e-mail: alexiherrerareyes@hotmail.com

La Libertad, 21/11/2023

DECLARACIÓN DE AUTORÍA

Yo VILLACRESES SUAREZ KEVIN GEOVANNY estudiante del octavo semestre de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura Unidad de Integración Curricular II, declaro la autoría del presente informe de investigación, de título "Estudio comparado a las normas de Ecuador, Venezuela y Perú con relación a las consecuencias jurídicas por el acceso no autorizado a sistemas informáticos", desarrollado en todas sus partes por el estudiante suscrito con apego a los requerimientos de la ciencia del derecho, la metodología de la investigación y las normas que regulan los procesos de titulación de la UPSE.

Atentamente

Kevin Geovanny Villacreses Suarez
CC. 1313927939

Celular: 0962944440
e-mail: villacreses16@gmail.com

TRIBUNAL

ANDRES ALEJANDRO ZULETA ARAQUE

Firmado digitalmente por ANDRES ALEJANDRO ZULETA ARAQUE
Fecha: 2024.01.31 09:42:34 -05'00'

Ab. Andrés Zuleta Araque, Mgt.

DOCENTE ESPECIALISTA

Ab. Victor Manuel Coronel Ortiz, Mgtr.

Director de la Carrera de Derecho

CRISTOBAL HOMERO MACHUCA REYES

Firmado digitalmente por CRISTOBAL HOMERO MACHUCA REYES
Fecha: 2024.01.30 09:38:34 -05'00'

Ab. Cristobal Machuca Reyes, Mgt.

DOCENTE TUTOR

Ab. Brenda Reyes Tomalá, Mgt.

DOCENTE GUIA DE LA UIC

DEDICATORIA

Este trabajo de investigación va dedicado a mi madre, padre y hermana, pilares fundamentales e irremplazables en mi crecimiento personal y académico; a mi abuela la Ing. Carmen Moran principal fuente de inspiración y motivación en mi vida académica; y demás amigos y familiares que me apoyaron en el transcurso de esta efímera, pero grata senda seguida.

AGRADECIMIENTO

Agradezco a todos los docentes que me apoyaron y compartieron su conocimiento y experiencias a lo largo de mi historial académico al igual que a mi tutor de tesis el Abg. Cristóbal Machuca. Así como a la Universidad Estatal Península de Santa Elena por el grato recibimiento mostrado desde el principio

ÍNDICE GENERAL

ÍNDICE DE TABLAS

INDICE DE ANEXOS

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
CARRERA DE DERECHO

"ESTUDIO COMPARADO A LAS NORMAS DE ECUADOR, VENEZUELA Y PERÚCON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS POR ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS"

Autor: Kevin Villacreses Suarez

Tutor: Dr. Cristóbal Machuca

RESUMEN

El avance tecnológico que ha experimentado nuestra sociedad en las últimas décadas ha generado una creciente relevancia para el derecho informático en la vida cotidiana de los ciudadanos. La integración cada vez mayor de la tecnología en el día a día de las personas conlleva desafíos significativos, especialmente en lo que respecta a la seguridad de los sistemas informáticos. Uno de los desafíos más apremiantes es el acceso no autorizado a estos sistemas, lo que plantea una problemática importante, ya que la información contenida en los mismos puede ser vulnerada. El presente proyecto de investigación tiene como objetivo realizar un análisis comparativo de las normativas vigentes que regulan el acceso no autorizado a sistemas informáticos en tres países: Ecuador, Perú y Venezuela. Para llevar a cabo este análisis, se utilizaron enfoques analíticos, descriptivos y detallados. Además, se abordaron temas fundamentales, como las definiciones de terminologías relacionadas con el derecho informático y las teorías de autores destacados en el campo. También se exploró el papel del conocimiento social en el derecho informático. Se puso un énfasis especial en evaluar la calidad de los ordenamientos jurídicos de los países objeto de estudio, resaltando tanto sus aciertos como sus falencias. Este enfoque permitió identificar de manera efectiva las diferencias en la severidad de las sanciones impuestas a quienes acceden sin autorización a sistemas informáticos en cada uno de estos países. En cuanto a la metodología empleada en esta investigación, se aplicaron métodos exegéticos, analíticos y de comparación jurídica para analizar la información contenida en las leyes, la doctrina y la bibliografía relacionada con el tema. Este estudio entrego resultados valiosos que permitirán comprender mejor la situación normativa de estos países en relación con el acceso no autorizado a sistemas informáticos y su impacto punitivo en las sanciones impuestas a quienes incurran en esta práctica

Palabras clave: Derecho informático, Acceso no autorizado, Sistemas informáticos, Análisis comparativo, Sanciones.

PENÍNSULA DE SANTA ELENA STATE UNIVERSITY
FACULTY OF SOCIAL AND HEALTH SCIENCES
LAW CAREER

ABSTRACT

The technological advancements that our society has experienced in recent decades have generated growing importance for cyber law in the daily day of citizens. The increasing integration of technology into people's day-to-day routines presents significant challenges, particularly regarding the security of computer systems. One of the most pressing challenges is unauthorized access to these systems, posing a substantial issue as the information they contain could be undertaken.

This research project aims to develop a comparative analysis of the current regulations governing unauthorized access to computer systems in three countries: Ecuador, Peru, and Venezuela. Analytical, descriptive, and detailed approaches were used to develop t this analysis. Fundamental topics were investigated, including definitions of terminologies related to cyber law and theories presented by prominent authors in the field of law. Furthermore, the study explored the role of social knowledge in cyber law. An emphasis was placed on evaluating the quality of the legal frameworks in the countries under study, highlighting their successes and shortcomings. This approach effectively identified differences in the severity of sanctions imposed on individuals who gain unauthorized access to computer systems in each nation.

Regarding the methodology employed in this investigation, explanation, analytical methods, and legal comparative analysis were applied to scrutinize information issued in-laws, doctrine, and literature associated with the subject. This study yielded valuable results that will better facilitate an understanding of the regulatory situation of these countries concerning unauthorized access to computer systems and the punitive impact of sanctions imposed on those engaging in such practices.

Keywords: Cyberlaw, Unauthorized access, Computer systems, Comparative analysis, Legal frameworks, Sanctions

INTRODUCCIÓN

En un contexto de avance tecnológico acelerado, el ámbito del derecho informático emerge como un pilar esencial para la protección de la sociedad en la era digital. La seguridad de los sistemas informáticos y la prevención del acceso no autorizado se han vuelto preocupaciones críticas, con amplias implicaciones legales. Este proyecto de investigación tiene como objetivo realizar un análisis comparativo de las normativas vigentes que regulan el acceso no autorizado a sistemas informáticos en tres países de América Latina: Ecuador, Perú y Venezuela.

En el capítulo I, titulado "El Planteamiento del Problema," se han identificado las cuestiones cruciales relacionadas con el acceso no autorizado a sistemas informáticos desde una perspectiva jurídica. Se ha señalado la importancia de examinar en profundidad la amplitud de este fenómeno, así como el poder sancionador del marco legal. Asimismo, se han presentado los objetivos estratégicamente definidos por el investigador, los cuales reflejan la visión rectora de este estudio en el contexto del derecho.

Para avanzar en la investigación, resulta fundamental la elaboración de los contenidos principales y secundarios predefinidos. Por lo tanto, en el capítulo II, se llevó a cabo una exhaustiva revisión de diferentes definiciones y teorías propuestas por diversos autores, las cuales contribuyen a una comprensión más profunda del tema de investigación. Asimismo, se destacó la relevancia de la sociedad en este contexto y se realizó un análisis detallado de la legislación vigente que regula la materia en cuestión en los tres países sudamericanos.

Por otro lado, en el capítulo III, denominado "Metodología de Investigación," se detallan las diferentes orientaciones que guían la labor investigativa. Esto incluye la elección del enfoque, el tipo de investigación y la metodología apropiada en la que las principales fuentes de análisis y discusión se basan para los diversos marcos legales y libros científico-jurídicos. Además, se considera la recopilación de indicadores y otros parámetros esenciales que facilitaron la comparación de las regulaciones relacionadas con el acceso no autorizado a sistemas informáticos en los países objeto de estudio.

Por último, en el capítulo IV, se aborda la presentación de los resultados y su posterior análisis. Se examinan las similitudes y diferencias identificadas entre las leyes en vigor en Ecuador, Venezuela y Perú. A partir de estos hallazgos, se construye un argumento que respalda la tesis a defender, evaluando su potencial validez o falsedad.

CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

La protección de datos personales y la seguridad de la información en el entorno digital plantean desafíos significativos en la actualidad. A medida que los avances tecnológicos continúan transformando nuestra sociedad, se hace necesario evaluar la legislación comparada en materia de delitos informáticos y protección de datos, con el fin de identificar similitudes y diferencias en la regulación del acceso no autorizado a sistemas informáticos y las medidas legales para prevenir y sancionar este tipo de delito.

En este contexto, se plantea la siguiente problemática: ¿Cuál es la efectividad de las normativas penales y de protección de datos relacionadas con el acceso no autorizado a sistemas informáticos en Ecuador, Venezuela y Perú?, ¿cómo se pueden mejorar las leyes y medidas de seguridad en línea en Ecuador a través del estudio comparado de estas regulaciones?

Para abordar esta problemática, se realizará un análisis exhaustivo de las legislaciones penales y de protección de datos de los países mencionados, centrándose en los artículos específicos que sancionan el acceso no autorizado a sistemas informáticos. Se identificarán las similitudes y diferencias en la regulación de este delito, así como las medidas legales establecidas para su prevención y sanción.

Asimismo, se examinarán las mejores prácticas identificadas en los países comparados y se propondrán recomendaciones para fortalecer la legislación y las medidas de seguridad en línea en Ecuador. Se considerarán aspectos como la adecuación de las penas establecidas, la colaboración público-privada en la prevención y detección de delitos informáticos, y la concienciación y educación en materia de seguridad digital. Es importante destacar que uno de los principales desafíos en nuestra sociedad actual se encuentra en la escasa difusión de información relacionada con la seguridad cibernética. Este problema afecta tanto a estudiantes de derecho como a abogados y al público en general. La rápida evolución de la información relacionada con la informática en comparación con otros ámbitos de nuestra sociedad genera una

creciente necesidad de regular conductas ilícitas que se llevan a cabo enel entorno digital, en particular, el acceso ilegal a sistemas informáticos. Este tipo de accesono solo representa un peligro para la entidad responsable del sistema en cuestión, sino también para las personas cuyos datos personales se encuentran almacenados en dicho sistema.

En el ámbito legal, se comenzará examinando la legislación ecuatoriana, la cual se encuentra establecida en el Código Orgánico Integral Penal. El Artículo 234 de dicho códigoestablece lo siguiente:

> Art. 234 - Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: Aquella persona que, sin autorización, acceda total o parcialmente aun sistema informático, telemático o de telecomunicaciones, o se mantenga dentro de los mismos en contra de la voluntad de quien posea el legítimo derecho, con el propósito de explotar de manera ilícita dicho acceso, modificar un portal web, desviar o redireccionar el tráfico de datos o voz, u ofrecer servicios que estos sistemas provean a terceros sin pagar a los proveedores de servicios legítimos, será sancionada con una pena privativa delibertad de tres a cinco años.

La legislación peruana cuenta con un enfoque más especializado en materia de seguridad informática, llegando incluso a poseer un código propio dedicado a este tipo de leyes. Aunqueno se mencionará a Venezuela en este contexto, es importante destacar que es consideradouno de los países con legislación informática más avanzada en Latinoamérica. En el caso de Perú, se cuenta con una Ley de Delitos Informáticos que regula diversos tipos de delitos cibernéticos, y en particular, en relación con el acceso no autorizado a sistemas informáticos,el Artículo 2 de dicha ley establece lo siguiente:

> Artículo 2 - Acceso ilícito: Aquel que, de manera deliberada e ilegítima, acceda total o parcialmente a un sistema informático, siempre y cuando se realice en violación de las medidas de seguridad establecidas para impedirlo, será sancionado con una pena privativade libertad no menor de uno ni mayor de cuatro años, así como con una multa de treinta a noventa días. Será sancionado con la misma pena aquel que acceda a un sistema informático excediendo los límites de la autorización.

Como principal punto de comparación con el Código Orgánico Integral Penal ecuatoriano, se puede observar que la legislación peruana establece una pena privativa de libertad menorque en Ecuador. Sin embargo, además de la privación de libertad, se impone una multa comosanción adicional en el caso peruano. Esta diferencia podría considerarse acertada, ya que las víctimas de este tipo de delitos también deberían recibir una compensación económica debido a la naturaleza delicada del delito en cuanto a la privacidad.

1.2 Formulación del problema

¿Cómo las legislaciones de Venezuela y Perú regulan la problemática virtual del acceso no consentido a los sistemas informáticos?

1.3 Objetivos Generales y Específicos

Objetivo general

Comparar las normativas penales y de protección de datos relacionados con el acceso no autorizado a sistemas informáticos en Ecuador, Venezuela y Perú, y evaluar las leyes y medidas de seguridad en línea en Ecuador mediante el estudio comparativo de las legislaciones de Perú y Venezuela.

Objetivos específicos

1. Realizar un análisis exhaustivo de la legislación de protección de datos en Ecuador, Venezuela y Perú, enfocándose en los artículos específicos que sancionan el acceso no autorizado a sistemas informáticos.
2. Identificar las similitudes y diferencias en la regulación del acceso no autorizado a sistemas informáticos en los tres países estudiados.
3. Examinar la efectividad de las medidas legales establecidas en cada país para prevenir y sancionar el acceso no autorizado a sistemas informáticos.

1.4 Justificación de la investigación

La presente investigación tiene como objetivo el análisis del acceso no concedido a los sistemas informáticos desde un enfoque legal por medio de un estudio comparado entre las legislaciones de Ecuador, Venezuela Y Perú.

Este trabajo permitirá obtener un punto de vista más globalizado respecto al acceso ilegal a los sistemas informáticos de modo que mediante el estudio de diferentes legislaciones se

puedan comparar y estudiar las normativas con el objetivo de analizar similitudes y diferencias entre las mismas.

El motivo que llevó a la realización de la presente investigación es la creciente problemáticaa la luz de la situación actual en casos de delitos informáticos y la necesidad de tener una normativa que cubra las diferentes conductas ilícitas que se pueden dar, tal y como lo es el tema del presente estudio.

Se pretende entonces mediante el método de investigación práctico que esta investigación sirva como referente tanto de estudio como de análisis para las personas que estudian y ejercen derecho, así como para quienes no lo hacen, con la finalidad de nutrir las diferentes investigaciones que se realizan en el Estado Ecuatoriano respecto al acceso ilícito a los sistemas informáticos.

1.5 Variables de la investigación

1: Acceso no autorizado a sistemas informáticos

1.6 Idea a defender

Las sanciones relativas al tipo penal con relación al tema a tratar respecto a la consecuencia jurídica que tiene el acceso no autorizado a los sistemas informáticos no son eficaces en comparación con las sanciones establecidas en las legislaciones de Perú y Venezuela.

CAPÍTULO II: MARCO REFERENCIAL

2.1 Marco teórico

2.1.2 Estudio doctrinario de derecho y Delitos informáticos

En la era digital y tecnológica de la actualidad, el derecho y los delitos informáticos se han convertido en temas de gran relevancia. La creciente dependencia de las tecnologías de la información y comunicación ha dado lugar a nuevos retos y desafíos legales que requieren un análisis y comprensión profundos. En este contexto, el presente estudio doctrinario se enfocará en el derecho informático y, específicamente, en los delitos informáticos.

En los tiempos modernos donde predominan las tecnologías de la información y comunicación, necesarios para satisfacer la demanda de servicios acorde al contexto de la sociedad, la evolución de la Ciencia de la Computación ha incursionado en el Derecho como facilitador de las labores de Abogados, Juristas, Servidores Públicos de la Administración de Justicia y público en general. En este sentido, la Ciencia del Derecho, como regulador de los fenómenos jurídicos derivados de la actividad del hombre en cualquier área, tuvo que

ocuparse de los mismos en consecuencia por la utilización de la informática en la vida diaria. (Aguilar, 2015, p. 19).

El derecho informático, también conocido como derecho de la informática o derecho de las tecnologías de la información, se refiere al conjunto de normas y principios legales que regulan el uso, acceso, almacenamiento, transmisión y protección de la información y los sistemas informáticos. Con el avance constante de la tecnología, este campo del derecho ha adquirido una importancia significativa, ya que abarca aspectos como la privacidad, la seguridad cibernética, la propiedad intelectual y la responsabilidad legal en el ámbito digital.

Uno de los fenómenos más relevantes y preocupantes en el ámbito del derecho informático son los delitos informáticos. Estos delitos, también conocidos como ciberdelitos o delitos cibernéticos, comprenden una amplia gama de actividades ilícitas que se llevan a cabo a través de las redes y sistemas informáticos. Estos pueden incluir desde el acceso no autorizado a sistemas o datos, hasta la difusión de malware, el fraude electrónico, el robo de información personal o financiera, entre otros. El estudio doctrinario sobre los delitos informáticos se enfocará en analizar y comprender las diferentes dimensiones de esta problemática.

Durante el desarrollo de este estudio se examinarán las leyes, convenios internacionales y jurisprudencia aplicables a los delitos informáticos, así como las teorías y enfoques doctrinarios desarrollados por expertos en el campo. Además, se analizarán casos emblemáticos y ejemplos concretos para ilustrar las diversas formas en que los delincuentes aprovechan las vulnerabilidades y debilidades del entorno digital para cometer actos ilícitos. El objetivo principal de este estudio doctrinario es profundizar en el conocimiento y la comprensión de los delitos informáticos desde una perspectiva jurídica.

1.2.2 Surgimiento del derecho informático

El surgimiento del Derecho Informático, de acuerdo con Téllez (2008), se remonta a 1949, cuando el juez Wiener publicó una obra que dedicó un capítulo al derecho y las comunicaciones, destacando la influencia de la cibernética en el ámbito jurídico, un fenómeno social de gran relevancia. Además, Loevinger (1949) propone que el siguiente paso en el progreso humano debe ser la transición de la teoría general del derecho hacia la jurimetría, término que se refiere a la sustitución del Juez por una computadora. Es importante señalar que estas primeras manifestaciones interdisciplinarias se centraron en las implicaciones informáticas del derecho, y se desarrollaron de manera adicional en la década de 1950.

El surgimiento de las primeras manifestaciones interdisciplinarias en el Derecho Informático en la década de 1950 marcó un hito importante en la evolución de la relación entre la tecnología y el ámbito jurídico. A medida que la sociedad se adentraba en la era digital, surgieron nuevas oportunidades, pero también desafíos, especialmente en el campo de la seguridad y la protección de la información. Con el avance de la tecnología y el crecimiento exponencial de las redes y sistemas informáticos, también se dio paso al auge de los delitos informáticos. El potencial de la informática para cometer actos ilegales atrajo la atención de los delincuentes, quienes comenzaron a aprovechar las vulnerabilidades de la tecnología para llevar a cabo diversas actividades criminales. Desde intrusiones y robo de datos hasta estafas en línea y ataques cibernéticos a gran escala, los delitos informáticos se han convertido en una preocupación creciente para gobiernos, empresas y ciudadanos en todo el mundo.

Es así que, a medida que la tecnología sigue avanzando, los delitos informáticos continúan evolucionando y adaptándose, lo que exige respuestas legales y medidas de seguridad cada vez más sofisticadas. La lucha contra estos delitos ha llevado a una mayor cooperación internacional y a la creación de leyes y regulaciones específicas para abordar esta problemática en el mundo digital.

2.2.3 Definición de los delitos informáticos según autores

Los autores Del Pino y Martín (2008) evalúan una definición del delito informático como aquel que se lleva a cabo con la ayuda de la informática o de técnicas relacionadas con esta área. Sin embargo, plantean una crítica ante ella, argumentando que se tiene una desventaja significativa al centrarse exclusivamente en la informática como medio para cometer estos delitos, sin tomar en cuenta que lo informático también puede ser el objeto de la infracción. La crítica sugiere que el enfoque de la definición es limitado, ya que se centra en el uso de la informática como una herramienta para cometer delitos, cuando no solo se trata de utilizar la informática para cometer acciones ilegales, sino que también hay casos en los que los delincuentes pueden atacar, dañar o robar datos, sistemas o recursos informáticos directamente.

El delito informático es un campo en constante evolución debido al crecimiento de la tecnología y la interconexión globa, y comprende una amplia variedad de actividades ilícitas, como el acceso no autorizado a sistemas, el robo de información, el fraude en línea y el ciberacoso. Al considerar tanto la informática como medio de comisión y como objeto de la infracción, se logra una visión más completa del alcance y la naturaleza de los delitos informáticos.

En adición, Rodríguez (1990) define que el delito informático se refiere a la realización de una acción que cumpla con los criterios establecidos para ser considerada como un delito. Esta acción debe llevarse a cabo mediante el uso de elementos informáticos y/o telemáticos, o bien, vulnerando los derechos del titular de un elemento informático, ya sea hardware o software. El concepto resalta la importancia de la tecnología informática y telemática en la comisión de estos delitos, e implica que cualquier actividad ilegal o contraria a las leyes, que se realice en el ámbito informático o telemático, puede ser clasificada como un delito informático. Esto abarca desde acciones como el acceso no autorizado a sistemas, el robo de información o manipulación de recursos informáticos, hasta la violación de derechos de los propietarios de estos elementos tecnológicos. Esta definición refleja la complejidad y la variedad de actividades delictivas que pueden llevarse a cabo en el ámbito digital. Además, resalta la importancia de considerar tanto los aspectos legales como tecnológicos al abordar los delitos informáticos. Esta comprensión más amplia es esencial para enfrentar y prevenir los desafíos que surgen en el mundo digital en constante evolución.

Adicionalmente, los autores Gonzáles, J., Bermeo, J., Villacreses, E. & Guerrero, J. (2018) definen los delitos informáticos como cualquier actividad delictiva que involucra el uso de computadoras para cometer actos ilegales, y agregan que "…estos pueden constituirse en nuevas formas penales donde se incluyen como elementos primarios al internet y a la computadora como instrumentos físicos…" (p. 180), es decir, estos delitos aprovechan las capacidades de las tecnologías informáticas para perpetrar acciones criminales. Además, mencionan que el delito informático ha dado lugar a nuevas formas penales debido a la aparición de internet y la computadora como instrumentos fundamentales en su comisión.

2.1.4 Importancia del derecho informático entorno a las nuevas tecnologías

La tecnología de la información ha brindado nuevas oportunidades para los delincuentes, permitiéndoles acceder a sistemas, redes y datos confidenciales de manera más sofisticada y encubierta. Internet, como una red global, se convierte en el escenario propicio para la coordinación y ejecución de estos delitos. Los delincuentes pueden conectarse, comunicarse y compartir información de manera instantánea y anónima, lo que dificulta su identificación y captura. Por otro lado, la computadora actúa como la herramienta esencial para llevar a cabo estas actividades delictivas, brindando la capacidad de realizar tareas complejas y automatizadas que facilitan el daño y la explotación de sistemas y personas. A medida que la sociedad se vuelve cada vez más dependiente de la tecnología y el mundo digital, el delito informático se ha convertido en una preocupación importante para las autoridades y el público en general. La necesidad de abordar este tipo de delincuencia ha llevado al desarrollo de leyes y regulaciones específicas para contrarrestar y prevenir los ataques informáticos.

La clasificación de los delitos informáticos permite comprender la diversidad de acciones delictivas que pueden ocurrir en el entorno digital. Estas clasificaciones pueden basarse en aspectos como el objetivo del delito (acceso no autorizado, daño a sistemas, fraude, etc.), la forma de comisión (mediante el uso de malware, ataques de phishing, ingeniería social, etc.), o el impacto que generan (daños económicos, violación de la privacidad, afectación de servicios públicos, etc.).

Por otra parte, las teorías y enfoques doctrinarios en el campo del derecho informático son fundamentales para comprender los aspectos técnicos, éticos y legales relacionados con los delitos informáticos. Estas teorías buscan analizar y explicar los factores subyacentes que contribuyen a la aparición y propagación de estos delitos, así como las implicaciones sociales y políticas que conllevan.

Algunas de las teorías y enfoques doctrinarios que se pueden abordar se incluye la teoría de sistemas, que analiza la interrelación entre tecnología, derecho y sociedad. Desde la perspectiva esta teoría se entiende que la tecnología, el derecho y la sociedad son componentes interdependientes de un sistema más amplio, siendo que se considera un sistema como "…una agrupación de componentes aislados, cuyas propiedades una vez reunidas pueden explicar las propiedades de todo el objeto…" (Génova y Guzmán, 1983, p. 17). Estos elementos se influyen y afectan mutuamente, y su estudio conjunto permite comprender cómo se adaptan y transforman en función de sus interacciones.

En primer lugar, la tecnología puede ser vista como un subsistema dentro del sistema social y legal. La tecnología actúa como un motor de cambio y desarrollo en la sociedad, creando nuevas oportunidades, desafíos y dilemas éticos, por ejemplo, el avance de la tecnología digital ha impulsado el surgimiento de nuevas formas de interacción social y de transacciones comerciales en línea, lo que a su vez ha requerido la adaptación y creación de marcos legales para regular dichas actividades.

El derecho, por su parte, se considera un subsistema normativo y regulador dentro del sistema social. El derecho establece las normas y principios que rigen las interacciones y relaciones entre las personas, así como entre las personas y la tecnología. En el contexto de la tecnología, el derecho desempeña un papel fundamental al establecer los marcos legales que buscan proteger los derechos individuales, garantizar la seguridad y privacidad de los usuarios, y promover la responsabilidad y la ética en el uso de la tecnología.

2.1.5 Interrelación entre la tecnologia, el derecho y la sociedad

Es importante tomar en cuenta que la sociedad se considera el sistema más amplio que engloba tanto a la tecnología como al derecho, e influye en la configuración de la tecnología y el desarrollo del marco legal a través de factores como los valores, las necesidades, las demandas y las aspiraciones de las personas. A su vez, la tecnología y el derecho tienen un impacto significativo en la sociedad, moldeando las relaciones sociales, las estructuras económicas, las prácticas culturales y la forma en que las personas interactúan entre sí.

Diversos autores han abordado la interrelación entre tecnología, derecho y sociedad, como Lawrence Lessig, Yochai Benkler y Bruno Latour.

La doctrina de Lessig (2009), ofrece una perspectiva valiosa para el análisis de la interrelación entre tecnología, derecho y sociedad en el marco de la tesis en cuestión, ya que ha desarrollado conceptos y teorías que exploran cómo el diseño arquitectónico de los sistemas tecnológicos puede impactar significativamente en las libertades individuales y en la estructura del poder en la sociedad contemporánea. Para este autor, el concepto central es el del código o arquitectura como una forma de regulación en la era digital. El código se refiere a las reglas y restricciones incorporadas en el diseño y funcionamiento de los sistemas tecnológicos, y tiene un impacto profundo en cómo las personas interactúan, se comunican y ejercen sus derechos en entornos digitales.

En su texto, Lessig distingue entre cuatro tipos de regulación en el entorno digital: el código, la ley, las normas sociales y el mercado. Cada uno de estos mecanismos de regulación desempeña un papel importante, pero también presenta limitaciones y riesgos. El código, en particular, tiene el potencial de ejercer un poder significativo al establecer los límites y las posibilidades de interacción en los sistemas tecnológicos.

Es importante mencionar que se advierte sobre la posibilidad de “corrupción del código". Esto implica que el diseño de los sistemas tecnológicos puede favorecer ciertos intereses y desfavorecer a otros, lo que puede tener un impacto en la distribución del poder y la igualdad de oportunidades. Por ejemplo, el diseño del código de una plataforma en línea puede influir en la privacidad y la autonomía de los individuos, ya sea fortaleciéndolas o socavándolas.

Otro concepto relevante en la doctrina de Lessig es el de "cultura libre", ya que se argumenta a favor de preservar y promover el acceso abierto a la información y el conocimiento en la era digital, cuestionando las restricciones excesivas impuestas por el derecho de autor y otras formas de propiedad intelectual que pueden limitar la creatividad, la innovación y el intercambio de ideas en la sociedad.

Al integrar esta doctrina en el análisis, se podrán examinar críticamente los aspectos de regulación, poder y libertad en la interacción entre tecnología y derecho. Este enfoque permitirá explorar cómo el diseño arquitectónico de los sistemas tecnológicos y las políticas legales influyen en la protección de los derechos individuales, la privacidad, la igualdad de oportunidades y el acceso a la información. Además, se podrán examinar los desafíos actuales y proponer posibles soluciones para lograr un equilibrio adecuado entre la innovación tecnológica y la protección de los valores fundamentales en la sociedad contemporánea.

Se plantea la idea, acorde a lo que dice Lessig (2001), de que la arquitectura de los sistemas tecnológicos tiene el poder de regular y controlar nuestras interacciones en el entorno digital, y esta regulación puede tener un impacto significativo en las libertades individuales y en la estructura misma del poder en la sociedad, por lo tanto, el entorno tecnológico actual, especialmente en relación con el internet y la digitalización, ha generado un desequilibrio en el poder entre los ciudadanos y los actores con influencia en el ámbito digital, como las grandes corporaciones y los gobiernos. Se debe destacar la importancia de comprender cómo las leyes y regulaciones pueden influir en esta dinámica de poder y cómo pueden afectar nuestros derechos y libertades en el entorno digital.

En su análisis, Lessig argumenta que las regulaciones y las leyes son cruciales para preservar y proteger los valores fundamentales en la era digital, como la privacidad, la libertad de expresión y la innovación. Sin embargo, también señala la necesidad de encontrar un equilibrio adecuado entre la regulación y la libertad, evitando tanto el exceso de regulación que puede sofocar la innovación y la creatividad, como la falta de regulación que puede llevar al abuso de poder y la violación de los derechos de los individuos.

En este sentido, este enfoque destaca la importancia de diseñar y aplicar políticas y regulaciones que promuevan un ecosistema digital saludable y equitativo, donde los derechos y las libertades de los individuos estén protegidos y donde exista un equilibrio adecuado entre el poder de los actores dominantes y los intereses de la sociedad en su conjunto.

Por su parte, la doctrina de Benkler (2006) se centra en el análisis de la relación entre la tecnología, el derecho y la sociedad desde una perspectiva socioeconómica. Desde un enfoque jurídico, el autor destaca la importancia de adaptar las regulaciones legales al contexto de la sociedad de la información y las tecnologías de la comunicación.

Este enfoque plantea que las regulaciones legales deben considerar el impacto de la tecnología en la forma en que se generan, comparten y utilizan los conocimientos y la información. En este sentido, aboga por un enfoque que equilibre la promoción de la innovación y la creatividad con la protección de los derechos individuales y la equidad en la distribución de los beneficios generados por la tecnología.

Desde el punto de vista jurídico, la doctrina de Benkler destaca la necesidad de una regulación flexible y adaptativa que tenga en cuenta la dinámica cambiante de la sociedad de la información. Propone que el derecho informático promueva la participación ciudadana, la diversidad y la innovación, y garantice la protección de los derechos fundamentales en el entorno digital.

En su análisis jurídico, Benkler examina cómo las regulaciones legales pueden fomentar la colaboración en red y la participación ciudadana, y cómo pueden abordar los desafíos relacionados con la propiedad intelectual, la privacidad, la libertad de expresión y otros derechos en el entorno digital.

En síntesis, el análisis jurídico de la doctrina de Benkler destaca la importancia de adaptar las regulaciones legales a la sociedad de la información, reconociendo los cambios socioeconómicos y tecnológicos que han surgido. Su enfoque jurídico propone una regulación flexible y adaptativa que promueva la participación ciudadana y la equidad en la sociedad digital, al tiempo que garantice la protección de los derechos fundamentales en el entorno digital.

La teoría del actor-red propuesta por Latour (2008) ofrece una perspectiva única y relevante para comprender los delitos informáticos. Esta teoría se enfoca en las interacciones complejas entre actores humanos y no humanos en la formación de redes sociotécnicas. En el contexto de los delitos informáticos, Latour sostiene que los sistemas tecnológicos y las infraestructuras digitales son actores en sí mismos, capaces de ejercer agencia y desempeñar un papel activo en la comisión de dichos delitos.

Los delitos informáticos, en su naturaleza y alcance, presentan desafíos únicos para el campo del derecho. La tecnología juega un papel fundamental en la comisión de estos delitos, y comprender su influencia en las interacciones humanas es esencial para abordar este fenómeno de manera eficaz.

Desde la perspectiva de Latour, los sistemas informáticos y las infraestructuras digitales se convierten en actores relevantes en el contexto de los delitos informáticos. Estos sistemas no solo facilitan la comisión de delitos, sino que también desempeñan un papel activo en su perpetuación. Por ejemplo, el malware y los bots automatizados actúan como actores no humanos que participan en actividades delictivas en línea.

La teoría del actor-red también destaca la importancia de comprender las interconexiones entre actores humanos y no humanos en la ciberdelincuencia. En este sentido, es necesario analizar las complejas interacciones entre hackers, ciberdelincuentes, sistemas informáticos y tecnologías en la formación de redes sociotécnicas criminales. Estas redes pueden involucrar tanto a actores humanos como a herramientas tecnológicas, y comprender su dinámica es esencial para una comprensión completa de los delitos informáticos.

Además, la teoría del actor-red plantea desafíos en la atribución de responsabilidad en los delitos informáticos. En lugar de centrarse exclusivamente en los perpetradores humanos, este enfoque amplía el espectro de responsabilidades para incluir a los sistemas tecnológicos y las infraestructuras digitales que facilitan los delitos. Esto implicaría reconocer la agencia de los sistemas tecnológicos y la necesidad de abordar la responsabilidad tanto en el nivel humano como en el nivel sociotécnico.

En resumen, la teoría del actor-red de Bruno Latour ofrece una perspectiva valiosa para comprender los delitos informáticos. Su enfoque en las interacciones entre actores humanos y no humanos y la consideración de la agencia de los sistemas tecnológicos y las infraestructuras digitales permiten una comprensión más completa de las dinámicas de los delitos informáticos y la atribución de responsabilidades en este ámbito.

2.1.6 La teoría de la neutralidad tecnológica

En el presente apartado se analizará de la teoría de la neutralidad tecnológica, un concepto ampliamente debatido en el ámbito legal y ético. Esta teoría plantea que las tecnologías en sí mismas son neutrales desde un punto de vista moral y que su impacto en la sociedad está determinado por el uso que se les dé por parte de los actores humanos. En el marco de esta investigación, se explorará las implicaciones de esta teoría en el ámbito del derecho y cómo influye en la toma de decisiones jurídicas relacionadas con la regulación de la tecnología.

La teoría de la neutralidad tecnológica sostiene que las tecnologías en sí mismas carecen de una carga moral inherente y que su valor y consecuencias dependen del contexto social y las decisiones de quienes las utilizan. Desde una perspectiva legal, esto implica que las leyes y regulaciones no deben favorecer ni discriminar tecnologías específicas en función de sus características intrínsecas, sino evaluar su impacto en función de cómo se utilizan y las consecuencias que generan en la sociedad.

En este sentido, la neutralidad tecnológica busca evitar la imposición de prejuicios normativos sobre las tecnologías, reconociendo que son las acciones humanas las que pueden dar lugar a efectos beneficiosos o perjudiciales. Desde un enfoque legal, esto implica que la responsabilidad recae en los usuarios y no en las propias tecnologías. Es decir, las acciones y decisiones de los individuos al utilizar la tecnología son las que determinan su impacto en la sociedad.

Sin embargo, es importante señalar que existen críticas y debates en torno a la teoría de la neutralidad tecnológica. Algunos argumentan que esta perspectiva pasa por alto el hecho de que las tecnologías pueden tener un diseño y una intencionalidad incorporada que influye en su impacto. Además, se sostiene que las tecnologías pueden transmitir o reforzar normas y valores, lo que puede dar lugar a la perpetuación de desigualdades y sesgos existentes en la sociedad. Colina (2023) expresa que:

> Sin suscribir el postulado ingenuo de la neutralidad tecnológica, hemos de decir que las redes sociales son multivalentes. Por una parte, ponen sobre el tapete el asunto de la invasión de la privacidad y de la vigilancia electrónica masiva y personalizada, potencial o efectivamente totalitaria, pero, por otra parte, también han hecho parte de primaveras políticas y de resistencias democráticas en el seno de países autoritarios y totalitarios.

En conclusión, la teoría de la neutralidad tecnológica es un concepto relevante en el ámbito legal y ético, que busca analizar el papel de la tecnología en la sociedad. Desde la perspectiva de un abogado, esta teoría plantea que las tecnologías en sí mismas no tienen una carga moral inherente y que su impacto está determinado por el uso que se les dé. No obstante, es fundamental considerar también el diseño de las tecnologías y las implicaciones sociales y éticas que puedan estar implícitas en su desarrollo y aplicación. En el ámbito jurídico, esto implica evaluar el impacto de la tecnología en función de su contexto y uso, así como tener en cuenta las implicaciones normativas y éticas en la toma de decisiones relacionadas con la regulación tecnológica.

2.1.7 Teoría del control

La teoría del control en el ámbito del derecho informático es un enfoque fundamental para abordar los desafíos legales y éticos relacionados con el uso de la tecnología y las actividades en línea. En un contexto de crecimiento exponencial de las tecnologías de la información y la comunicación, se ha producido un aumento significativo en los delitos informáticos, ataques cibernéticos y violaciones a la privacidad. Ante esta realidad, la teoría del control postula la necesidad de establecer mecanismos efectivos de regulación y supervisión para mitigar y sancionar estas conductas.

Desde una perspectiva jurídica, la teoría del control implica la promulgación de leyes y regulaciones que establezcan estándares claros para la seguridad de la información, la protección de datos personales y la responsabilidad en el uso de la tecnología. Es esencial contar con un marco normativo sólido que defienda los derechos fundamentales y la privacidad de los individuos, al tiempo que establezca pautas para una conducta ética en el ámbito digital.

La implementación de medidas legales y técnicas adecuadas se vuelve fundamental para garantizar la seguridad y la integridad de los sistemas y redes informáticas. Esto implica el desarrollo de herramientas de detección y prevención de intrusos, sistemas de encriptación, autenticación de usuarios y técnicas de protección contra malware y ataques cibernéticos.

Sin embargo, la teoría del control no se limita únicamente a la imposición de restricciones y sanciones. También busca fomentar la conciencia y la educación en materia de seguridad informática, así como promover prácticas éticas en el uso de la tecnología. La capacitación de usuarios, la promoción de la responsabilidad individual y la colaboración entre los actores involucrados, como los proveedores de servicios, las empresas y los usuarios finales, son aspectos clave para el éxito de este enfoque.

En conclusión, la teoría del control en el ámbito del derecho informático se presenta como un instrumento esencial para enfrentar los retos legales y éticos derivados del uso de la tecnología en la sociedad actual. Mediante la implementación de medidas de seguridad, protección de datos y promoción de prácticas éticas, se pretende regular y supervisar de manera efectiva las acciones y comportamientos en línea, salvaguardando los derechos fundamentales y la privacidad de los individuos.

la teoría de la neutralidad tecnológica, que busca establecer principios legales que se apliquen de manera equitativa a cualquier tecnología; y la c, que enfatiza la necesidad de implementar medidas de seguridad y regulación para prevenir los delitos informáticos.

2.1.7 El peso del desconocimiento social respecto al derecho informático y el acceso no autorizado a los sistemas informáticos

La evolución tecnológica en el siglo XXI ha dado lugar a un entorno digital interconectado que permea todos los aspectos de la vida moderna. Sin embargo, esta transformación también ha traído consigo desafíos legales y éticos, particularmente en el ámbito del derecho informático y la ciberseguridad. La ignorancia generalizada sobre estos asuntos, junto con la falta de comprensión de sus implicaciones legales, ha generado un panorama en el que el acceso no autorizado a sistemas informáticos es tratado con demasiada ligereza.

2.1.8 Desconocimiento y Subestimación

A pesar de la existencia de estas leyes, el desconocimiento generalizado sobre el derecho informático y la ciberseguridad ha llevado a una subestimación de la gravedad de las acciones que involucran el acceso no autorizado. La falta de familiaridad con los términos legales y las posibles consecuencias legales ha llevado a muchas personas a creer erróneamente que ciertos actos digitales son inofensivos o que carecen de repercusiones jurídicas. Esta creencia errónea puede llevar a la perpetuación de prácticas riesgosas y potencialmente ilegales.

Indudablemente, la sociedad contemporánea se encuentra en un punto crucial en lo que respecta al desconocimiento del derecho informático y el acceso no autorizado a sistemas informáticos. Este fenómeno ejerce una influencia significativa en la manera en que las personas interactúan y se desenvuelven en el entorno digital. La importancia de abordar esta cuestión radica en la profunda interconexión entre la sociedad y la tecnología, así como en las repercusiones legales y éticas que surgen de la ignorancia en este ámbito.

El tejido social actual se encuentra entrelazado con la tecnología en una magnitud nunca antes vista. Desde las comunicaciones y el comercio hasta la educación y el entretenimiento, la tecnología informática ha permeado todas las esferas de la vida cotidiana. Sin embargo, a medida que estas herramientas digitales se vuelven más ubicuas, también crece la necesidad de comprender las implicaciones legales que conllevan. El acceso no autorizado a sistemas informáticos puede resultar en la exposición de datos personales, el compromiso de la privacidad y, en casos extremos, la alteración de infraestructuras críticas. El desconocimiento sobre cómo prevenir y responder a estas amenazas puede exponer a individuos y organizaciones a riesgos innecesarios.

Desde un enfoque legal, la sociedad desinformada sobre el derecho informático corre el riesgo de actuar en violación de las leyes sin tener conocimiento de ello. Los delitos informáticos, como el acceso no autorizado, pueden tener consecuencias penales y civiles sustanciales. La falta de comprensión de las normativas vigentes puede llevar a la subestimación de las acciones y a la creación de una cultura de impunidad en línea. Esto, a su vez, puede socavar la confianza en las transacciones digitales y en la infraestructura tecnológica en general.

El aspecto ético es igualmente crucial en este contexto. La sociedad debe reconocer la importancia de respetar la privacidad y la propiedad de otros en el mundo digital, al igual que en el mundo físico. El desconocimiento sobre el acceso no autorizado puede llevar a la invasión de la privacidad de individuos y a la explotación de vulnerabilidades en sistemas informáticos. La educación en este ámbito no solo imparte conocimientos legales, sino que también fomenta una ética digital que promueve la responsabilidad y el respeto en línea.

2.1.9 Impacto en la Sociedad

Desde una perspectiva sociológica, el desconocimiento sobre el derecho informático también influye en la formación de una cultura digital que no valora adecuadamente la ciberseguridad y la privacidad. El énfasis en la conveniencia y la rapidez en las interacciones en línea puede llevar a la negligencia en la protección de datos personales y a la participación inadvertida en actividades ilegales. La falta de educación sobre estos temas perpetúa un ciclo en el que las personas pueden ser víctimas o perpetradores de infracciones cibernéticas sin siquiera darse cuenta. Indudablemente, el impacto social derivado del desconocimiento sobre el derecho informático y el acceso no autorizado a sistemas informáticos es un factor de gran envergadura que permea múltiples aspectos de la sociedad contemporánea. El amplio alcance de este fenómeno se traduce en consecuencias tanto a nivel individual como colectivo, influyendo en la percepción de la ciberseguridad, el comportamiento digital y las relaciones interpersonales.

A nivel individual, el desconocimiento de las implicaciones legales y éticas del acceso no autorizado a sistemas informáticos puede tener efectos perjudiciales significativos. Los individuos pueden caer presa de malentendidos sobre lo que constituye una actividad legal en línea y pueden, inadvertidamente, violar las leyes informáticas. Esto puede llevar a sanciones legales y daños reputacionales que afectan la vida personal y profesional. Además, el desconocimiento puede exponer a las personas a riesgos de seguridad y privacidad, como el robo de identidad, la suplantación digital y la divulgación no deseada de información personal.

A nivel colectivo, el impacto es igualmente palpable. La falta de comprensión del acceso no autorizado a sistemas informáticos puede dar lugar a la normalización de prácticas digitales arriesgadas y potencialmente ilegales. Esto crea un entorno en línea donde la ciberseguridad es relegada a un segundo plano, generando una cultura de complacencia que socava los esfuerzos por mantener la integridad de los sistemas digitales. La sociedad se enfrenta a la posibilidad de caer en un ciclo de infracciones digitales, donde la falta de conocimiento perpetúa la participación en actividades que pueden tener daños colaterales a gran escala.

Además, el desconocimiento sobre el derecho informático y el acceso no autorizado también tiene un impacto en la confianza en las relaciones digitales. La comunicación y las transacciones en línea se basan en la creencia de que los sistemas son seguros y que las interacciones son legítimas. Sin embargo, el desconocimiento puede socavar esta confianza y generar escepticismo sobre la autenticidad y la seguridad de las comunicaciones digitales. Esto puede dificultar la adopción de nuevas tecnologías y limitar el potencial de la economía digital.

En última instancia, el impacto social del desconocimiento en el ámbito del derecho informático y el acceso no autorizado a sistemas informáticos resalta la necesidad urgente de abordar este tema. A través de la educación y la concientización, es posible mitigar los efectos negativos del desconocimiento, empoderando a los individuos para tomar decisiones informadas y éticas en el entorno digital. La creación de una sociedad informada y responsable en relación con la ciberseguridad no solo beneficia a nivel personal, sino que también contribuye a un ciberespacio más seguro y confiable para todos.

Educación y Concientización

La necesidad de abordar el peso del desconocimiento social en relación con el derecho informático y el acceso no autorizado a sistemas informáticos es crucial. Las instituciones educativas, junto con organismos gubernamentales y organizaciones de la sociedad civil, deben implementar programas de educación y concientización. Estos programas deben ofrecer información detallada sobre las leyes vigentes, las implicaciones legales y éticas de las acciones digitales, así como medidas para proteger la seguridad y la privacidad en línea

En última instancia, el desconocimiento social sobre el derecho informático y el acceso no autorizado a sistemas informáticos plantea un desafío multifacético que requiere atención inmediata. A través de la educación y la concientización, es posible fomentar una sociedad informada y ética en el ámbito digital, donde la ciberseguridad sea una prioridad y las interacciones en línea se realicen con responsabilidad y conocimiento de las implicaciones legales.

Indudablemente, la promoción de la educación y concientización en relación con el desconocimiento sobre el derecho informático y el acceso no autorizado a sistemas informáticos reviste un fundamento jurídico sólido y esencial en la sociedad contemporánea. Este enfoque se erige como una vía efectiva para prevenir la comisión de delitos cibernéticos, fomentar una cultura de ciberseguridad y salvaguardar los derechos y la privacidad de los individuos en el ámbito digital.

Desde una perspectiva jurídica, la educación y concientización en temas relacionados con el derecho informático tienen sus raíces en los principios fundamentales de la justicia y el imperio de la ley. En una sociedad democrática y basada en el Estado de derecho, se espera que los ciudadanos conozcan y respeten las leyes que rigen su comportamiento, tanto en el mundo físico como en el digital. El acceso no autorizado a sistemas informáticos puede ser un delito que conlleva consecuencias legales significativas, y el desconocimiento de estas leyes no exime a los individuos de su responsabilidad. Por lo tanto, la educación y concientización en este ámbito tienen un fundamento en la promoción de la equidad y la justicia, garantizando que todos los ciudadanos tengan acceso a la información necesaria para cumplir con las leyes y evitar conductas ilegales.

Además, la educación y la concientización también están en línea con la noción de que la prevención es preferible a la persecución en el sistema legal. Al proporcionar a las personas un conocimiento sólido sobre los límites legales en el mundo digital y los peligros asociados con el acceso no autorizado a sistemas informáticos, se está estableciendo una base para evitar que se cometan delitos cibernéticos. Esto no solo alivia la carga del sistema judicial, sino que también contribuye a la protección de los derechos individuales y la integridad de los sistemas digitales.

La educación y concientización también se alinean con el concepto de "ignorantia legis non excusat" o "la ignorancia de la ley no excusa". Este principio legal establece que el desconocimiento de las leyes no exime a una persona de su cumplimiento. En el contexto del acceso no autorizado a sistemas informáticos, esta noción cobra especial relevancia. La educación y concientización son herramientas que permiten a las personas cumplir con la ley de manera efectiva, evitando acciones que puedan ser perjudiciales para ellos mismos y para otros.

En conclusión, la importancia de la educación y concientización respecto al desconocimiento sobre el derecho informático y el acceso no autorizado a sistemas informáticos se asienta en fundamentos jurídicos sólidos. Estos principios legales subrayan la necesidad de que los ciudadanos comprendan y cumplan con las leyes relacionadas con la ciberseguridad y el acceso digital. La educación y la concientización son medios esenciales para prevenir delitos cibernéticos, promover una cultura de ciberseguridad y garantizar el respeto de los derechos individuales en el entorno digital.

2.2 Marco Legal

2.2.1 Código Orgánico Integral Penal de Ecuador

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.

2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

El primer párrafo del artículo 234 establece como una infracción grave la acción de acceder sin autorización a un sistema informático, telemático o de telecomunicaciones, ya sea en su totalidad o en parte, en contra de la voluntad de quien tiene un legítimo derecho sobre dicho sistema. Desde una perspectiva legal, esto se considera una invasión a la propiedad o la posesión de un bien jurídico, específicamente un sistema tecnológico.

El artículo establece una pena privativa de la libertad de tres a cinco años para esta conducta. La gravedad de la sanción refleja el reconocimiento de la importancia de proteger la integridad de los sistemas informáticos y la confidencialidad de la información almacenada en ellos.

El segundo párrafo del artículo 234 se enfoca en sancionar específicamente el acceso no autorizado con fines de explotación ilegítima. Esta explotación ilegítima puede manifestarse de diversas formas, como la modificación de un portal web, el desvío o redirección del tráfico de datos o voz, o la prestación de servicios que los sistemas proporcionan a terceros sin pagar a los proveedores legítimos de servicios.

La sanción para esta conducta es nuevamente una pena privativa de la libertad de tres a cinco años. Esto refleja la gravedad de la explotación ilegítima de sistemas tecnológicos y la necesidad de prevenir actividades fraudulentas en línea.

Puntos clave:

1. Gravedad de la pena: La pena de tres a cinco años de prisión es significativa y refleja la seriedad con la que la ley aborda el acceso no autorizado a sistemas tecnológicos. Esta gravedad busca disuadir a los infractores y proteger la integridad de los sistemas y la confidencialidad de la información almacenada en ellos. La privación de la libertad es una sanción seria y esencialmente priva al condenado de su libertad durante un período sustancial.

2. Proporcionalidad: La pena se considera proporcional a la gravedad de la infracción. El acceso no autorizado a sistemas informáticos puede tener un impacto significativo en la seguridad de datos y la privacidad de las personas, por lo que es coherente con la importancia de proteger estos activos digitales.

Es decir que el artículo 234 del Código Orgánico Integral Penal se enfoca en la protección de la propiedad y la seguridad de los sistemas informáticos y tecnológicos. Establece sanciones significativas para aquellos que acceden sin autorización a estos sistemas, así como para aquellos que realizan actividades ilegítimas o fraudulentas una vez que han obtenido acceso. Este enfoque legal tiene como objetivo disuadir el acceso no autorizado y garantizar la integridad de los sistemas y la confidencialidad de la información almacenada en ellos, contribuyendo a la seguridad y protección de los activos tecnológicos en la sociedad moderna.

2.2.2 Ley de delitos informáticos de Perú.

> Artículo 2. Acceso ilícito El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

El artículo 2 establece disposiciones legales relacionadas con el acceso ilícito a sistemas informáticos. Desde una perspectiva legal, este artículo se analiza de la siguiente manera:

El artículo define el delito de acceso ilícito como el acto deliberado e ilegítimo de acceder, total o parcialmente, a un sistema informático. Este acceso ilícito se castiga cuando se realiza con la vulneración de medidas de seguridad establecidas para impedirlo. La ilegitimidad del acceso se basa en la falta de autorización por parte del propietario o responsable del sistema informático en cuestión.

La sanción establecida por el artículo para este delito es una pena privativa de libertad no menor de un año ni mayor de cuatro años, además de una multa que oscila entre treinta y noventa días. Este castigo refleja la seriedad con la que la ley considera la violación de la seguridad de sistemas informáticos y busca disuadir este tipo de conducta.

El artículo también aborda la situación en la que una persona accede a un sistema informático, pero lo hace excediendo los límites de la autorización concedida. Esto implica que, aunque inicialmente puede haber tenido cierto grado de autorización, la conducta se convierte en ilícita cuando se sobrepasan esos límites establecidos.

La pena aplicable a esta situación es la misma que para el acceso ilícito mencionado anteriormente: una pena privativa de libertad no menor de un año ni mayor de cuatro años y una multa de treinta a noventa días.

1. Multa en casos de acceso ilícito:

El artículo 2 establece que, en casos de acceso ilícito a un sistema informático, la sanción comprende una pena privativa de libertad no menor de un año ni mayor de cuatro años, así como una multa de treinta a noventa días. Esta multa es un componente significativo de la sanción impuesta al infractor y merece una consideración detallada.

2. Función de la multa:

La multa tiene varias funciones dentro del sistema legal:

a. Punitiva: La multa impone una carga financiera al infractor como una forma de castigo adicional a la pena de prisión. Busca disuadir al infractor y a otros de cometer delitos similares en el futuro.

b. Compensatoria: La multa puede destinarse a compensar a la víctima o a la sociedad por los daños causados por el delito. En este caso, podría considerarse como una forma de resarcimiento por los costos incurridos en la reparación de los daños causados por el acceso ilícito.

c. Preventiva: La multa también puede servir como un medio para recuperar los beneficios obtenidos ilícitamente por el infractor, lo que puede ayudar a desincentivar la realización de actos ilegales.

3. Rango de la multa:

El artículo establece un rango específico para la multa, que va desde treinta a noventa días. Este rango permite cierta flexibilidad en la determinación de la multa, teniendo en cuenta las circunstancias específicas de cada caso. La cantidad exacta dentro de este rango dependerá de la gravedad de la infracción, la capacidad económica del infractor y otros factores relevantes.

4. Importancia de la multa económica:

La multa económica es un componente esencial en la aplicación de la ley en casos de acceso ilícito a sistemas informáticos. No solo cumple una función sancionadora, sino que también puede ser una fuente de ingresos para el sistema legal y contribuir a la reparación de daños causados. Su imposición adecuada es fundamental para garantizar que el castigo sea proporcional al delito y para fomentar la legalidad y la ciberseguridad en un entorno tecnológico en constante evolución.

Es decir que la multa económica en el artículo 2 desempeña un papel importante en la sanción de casos de acceso ilícito a sistemas informáticos. Cumple diversas funciones legales, incluida la punitiva, compensatoria y preventiva, y su rango variable permite una adaptación a las circunstancias específicas de cada caso. La imposición y ejecución adecuadas de la multa son fundamentales para garantizar la eficacia del sistema legal en la protección de la seguridad informática y la disuasión de actividades ilegales en este ámbito.

2.2.3 Ley Especial Contra los Delitos Informáticos de Venezuela

> Artículo 6. Acceso indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

El texto legal en cuestión aborda el delito de acceso indebido a sistemas que utilizan tecnologías de información. A continuación, se presenta un análisis legal en tercera persona del artículo:

1. Delito de acceso indebido:

El artículo define el delito de acceso indebido como la acción de acceder, interceptar, interferir o utilizar un sistema que utiliza tecnologías de información sin la debida autorización o excediendo la autorización otorgada. Esta disposición legal reconoce la importancia de proteger la integridad de los sistemas informáticos y de información en un entorno tecnológico cada vez más relevante.

2. Sanciones establecidas:

El artículo establece las sanciones para este delito. En primer lugar, se impone una pena de prisión que varía de uno a cinco años. Esta pena privativa de libertad refleja la gravedad del delito y busca disuadir a los infractores de cometer acciones de acceso indebido a sistemas tecnológicos.

Además de la pena de prisión, el artículo también prevé una multa económica. El rango de la multa va desde diez hasta cincuenta unidades tributarias. Esta multa es un componente importante de la sanción y cumple varias funciones legales, incluida la punitiva, la compensatoria y la preventiva.

3. Importancia de la multa:

La multa desempeña un papel significativo en la sanción de este delito. Además de la pena de prisión, la multa se impone como un medio adicional de castigo y como una forma de resarcir a la sociedad o la víctima por los daños causados por el delito. También puede tener un carácter preventivo al desincentivar la comisión de actos ilegales.

4. Flexibilidad en el rango de la multa:

El rango de la multa varía entre diez y cincuenta unidades tributarias. Esta flexibilidad permite que las sanciones se adapten a las circunstancias específicas de cada caso. La cantidad exacta de la multa se determina teniendo en cuenta la gravedad de la infracción, la capacidad económica del infractor y otros factores relevantes.

5. Protección de sistemas de información:

El artículo 6 tiene como objetivo principal proteger la seguridad y la confidencialidad de los sistemas de información y tecnología. El acceso indebido a estos sistemas representa una amenaza para la integridad de los datos y la propiedad intelectual. Por lo tanto, el artículo establece sanciones proporcionales para prevenir y castigar estas conductas ilícitas.

Desde una perspectiva legal, este análisis destaca los siguientes aspectos relacionados con la forma de acceder al sistema:

- Acceder: Esto implica la entrada no autorizada a un sistema que utiliza tecnologías de información. El acceso sin la debida autorización constituye una infracción en sí misma, y el artículo se aplica a aquellos que ingresan a sistemas sin permiso.

- Interceptar: Esta acción involucra la captura o el monitoreo no autorizado de datos o comunicaciones que se están transmitiendo a través de un sistema. La interceptación ilegal de información también se considera una violación.

- Interferir: La interferencia implica modificar, perturbar o afectar negativamente el funcionamiento normal de un sistema. Esta acción puede causar daños o perjuicios al sistema o a los datos contenidos en él.

- Usar: El uso no autorizado de un sistema, incluso si se tiene acceso legítimo, puede ser una infracción si se excede la autorización otorgada. Esto abarca el uso indebido de la información o recursos del sistema.

Gravedad de las Sanciones: El artículo establece sanciones significativas para este delito. La pena de prisión de uno a cinco años refleja la seriedad del delito y busca disuadir a los infractores de cometer actos ilícitos relacionados con sistemas que utilizan tecnologías de información. Además, se prevé una multa, que varía desde diez hasta cincuenta unidades tributarias, como sanción adicional.

Es decir que el artículo 6 aborda el delito de acceso indebido a sistemas de tecnologías de información y establece sanciones penales y económicas. La multa es un componente esencial de la sanción, con funciones punitivas, compensatorias y preventivas, y su rango variable permite la adaptación a las circunstancias específicas de cada caso. La imposición adecuada de la multa es fundamental para garantizar la eficacia del sistema legal en la protección de la seguridad informática y la disuasión de actividades ilegales en este ámbito.

2.3 Marco Conceptual.

El Derecho Comparado: el Derecho Comparado es método de investigación pues exige recurrir a procedimientos y estrategias para confrontar el propio derecho con el foráneo, detectando conexiones causales o relaciones subyacentes entre las tradiciones o familias jurídicas y con ello, similitudes o diferencias. (Cáceres, 2018)

ignorantia legis non excusat: Hace referencia a que una vez promulgadas las leyes, éstas se presumen conocidas por todos. Esta situación se basa en dos principios generalmente admitidos: a) a nadie le es permitido ignorar las leyes: “nemine jus ignorare licet”; b) se presume que todos las conocen, por lo cual, aunque alguno las ignore, le obligan como si no las ignorara: “nemo jus ignorare consetur; ignorantia legis neminem excusat”. DE HECHO. El desconocimiento de una relación, circunstancia o situación material cuando tiene efectos jurídicos en el supuesto de llegar a saber la verdad quien procedió ignor ndola. DE LA LEY. v. Ignorancia de derecho. INEXCUSABLE. (Cabanellas, 2006)

Sistema informático: Los sistemas informáticos son los sistemas encargados de recibir, guardar y procesar información para posteriormente entregar resultados a partir de ello. Son sistemas complejos y presentes en diversos ámbitos, ya que engloba a todo aquello que contiene una división física (hardware) y otra lógica (software). (Chavez)

Delitos informáticos: Davara Rodríguez define al Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software. (Pino, 2016)

Arquitectura de la Información: El término "Arquitectura de la Información" (AI) fue utilizado por primera vez por Richard Saul Wurman en 1975, quién la define como el estudio de la organización de la información con el objetivo de permitir al usuario encontrar su vía de navegación hacia el conocimiento y la comprensión de la información. (Fernández & Hassan Montero, 2003)

Jurimetría: Jurimetría es una herramienta de analítica jurisprudencial que permite definir la estrategia procesal más idónea para el éxito del caso, a través de indicadores gráficos interactivos, basados en el análisis cognitivo de millones de decisiones judiciales. (Comparador LegalTech , s.f.)

Teoría de Sistemas: Se conoce como Teoría de sistemas o Teoría General de Sistemas al estudio de los sistemas en general, desde una perspectiva interdisciplinaria, o sea, que abarca distintas disciplinas.

Su aspiración es identificar los diversos elementos y tendencias identificables y reconocibles de los sistemas, o sea, de cualquier entidad claramente definida, cuyas partes presentan interrelaciones e interdependencias, y cuya suma es mayor que la suma de sus partes. (Editorial Etecé, 2021)

Imperio de la ley: En sentido amplio, la expresión imperio de la ley alude a un ideal regulativo sobre el ejercicio del poder. De acuerdo con dicho ideal, la legitimidad del poder reside en que su actuación se ajuste a lo establecido por normas jurídicas preconstituidas. Con todo, la expresión adolece de un elevado nivel de indeterminación semántica; tan amplio como la propia noción de ley o Derecho. (María, 2013)

CAPÍTULO III: MARCO METODOLOGICO

3.1 Diseño de investigación y tipo de investigación

La presente investigación tiene como principal enfoque de investigación el método cualitativo, debido que este permite y pretende la realización de un análisis amplio, así como la elaboración de conclusiones relevantes sobre la problemática a tratar, mediante el uso del derecho comparado entre las normativas de Ecuador, Perú y Venezuela como pilar principal en la investigación, de modo que se puedan analizar las formas en la cual cada una de estas legislaciones tratan el delito de acceso no autorizado hacia los sistemas informáticos con la finalidad de lograr obtener resultados investigativos que ayuden a evaluar la efectividad de las normas penales que regulan este tipo penal en el Ecuador.

A través de los instrumentos que sirven como fuente de información correspondiente para la realización del correspondiente estudio comparado de normas como lo son las propias normativas internacionales, así como las respectivas referencias bibliográficas para el desarrollo del trabajo, de modo que a partir de la ejecución de técnicas de investigación se pueda ayudar a lograr los objetivos planteados

3.2 Recolección de información

El presente texto tiene como factor fundamental el tipo de investigación exploratorio, debido a que la información recopilada ayuda a determinar la efectividad de la sanción en base a lo que determinan en la normativa de Venezuela y Perú, comparada con lo establecido en la normativa de Ecuador en el Código Orgánico Integral penal en su artículo 234 referente al acceso no consentido a un sistema informático.

Población

La población es un elemento crucial en cualquier investigación, ya que define el conjunto total de individuos o elementos que serán objeto de estudio. En la presente investigación la selección adecuada y representativa de la población es fundamental para garantizar la validez de los

resultados obtenidos. Una población bien definida permite contextualizar el problema de investigación y proporciona la base para realizar inferencias precisas sobre el fenómeno en cuestión.

TABLA 1: Población

PAÍS	DETALLE	N°
Ecuador	Código orgánico integral penal	1
Perú	Ley de delitos informáticos	1
Venezuela	Ley especial contra los delitos informáticos	1

Elaborado por: Villacreses Suarez Kevin Geovanny (2023).

Esta investigación no requiere muestra debido a la naturaleza de la misma, al enfocarse principalmente en la comparación de elementos normativos existentes. En consecuencia, se procederá a analizar los elementos normativos mencionados con la finalidad de recolectar datos de los mismos en lugar de recolectar datos de una muestra representativa de la población.

Métodos, técnicas e instrumentos

Los métodos de investigación son fundamentales para obtener conocimiento sistemático y confiable sobre un tema específico. Estos métodos proporcionan las herramientas y estrategias necesarias para recolectar, analizar y comprender datos de manera objetiva y rigurosa. En el contexto académico y científico, existen varios enfoques de investigación, cada uno con sus propias características y objetivos. En esta investigación se emplearán tres métodos investigativos fundamentales: el método exegético, el método analítico y el método comparativo.

Método exegético

Este enfoque implica un estudio detallado de los diferentes textos legales, se procederá con la utilización de este método para poder realizar una comparación de los diferentes cuerpos legales en Ecuador, Perú y Venezuela que traten el principal tema de estudio de esta investigación siendo este el acceso no concedido a los sistemas informáticos, de modo que se comparará las diferencias entre la propia definición del delito, sanciones aplicables y otros aspectos relevantes.

Método analítico

El método analítico acarrea un análisis detallado de los elementos que componen la legislación, tal y como son los principios fundamentales, derechos, obligaciones, sanciones y otros aspectos legales relevantes.

Al utilizar el método analítico se pueden realizar comparaciones sistemáticas de las diferentes legislaciones involucradas con la finalidad de obtener los objetivos y propósitos de cada legislación, de igual manera ayuda en la obtención de resultados que demuestren notablemente las similitudes y diferencias entre los cuerpos legales analizados, facilitando la observación de posibles grietas normativas o áreas a mejorar en la legislación de cada país.

Método comparativo jurídico

El método comparativo jurídico es una estrategia empleada en el campo del derecho que tiene como objetivo examinar y analizar las similitudes y disparidades existentes entre los sistemas legales de distintos países o regiones. Esta técnica implica una comparación detallada de leyes, normativas, procesos judiciales y fallos judiciales, con el fin de identificar tendencias compartidas, diferencias relevantes y potenciales soluciones a problemáticas legales afines.

La elección del método comparativo jurídico para abordar el tema de "Estudio comparado a las normas de Ecuador, Venezuela y Perú con relación a las consecuencias jurídicas por acceso no autorizado a sistemas informáticos" se justifica por razones fundamentales que enriquecerán la investigación y sus conclusiones. Principalmente al tratarse de un tema relacionado con delitos informáticos y aspectos jurídicos, el método comparativo permitirá obtener una visión integral y detallada de cómo estos tres países enfrentan y regulan el acceso no autorizado a sistemas informáticos. Al comparar las leyes, normas y procedimientos legales aplicados en cada jurisdicción, será posible identificar tanto similitudes como diferencias, lo que proporcionará una comprensión más completa de las estrategias legales adoptadas por cada país.

Técnicas e instrumentos de la investigación

Las técnicas e instrumentos de investigación son herramientas y procedimientos utilizados para recopilar datos y obtener información relevante en un proceso de investigación. Las técnicas se refieren a los métodos generales empleados, mientras que los instrumentos son los medios concretos utilizados para aplicar esas técnicas y obtener datos específicos. Su correcto uso es fundamental para obtener conclusiones precisas y respaldadas por evidencia en la investigación.

Técnicas de investigación

La presente investigación se enmarca en el campo del derecho comparado y, en virtud de la complejidad y amplitud inherentes de los sistemas legales que se estudian, se hace uso de las técnicas de fichaje como una herramienta esencial para llevar a cabo un análisis detallado y exhaustivo. Los métodos de investigación empleados en este estudio son el analítico, el exegético y la comparación jurídica, los cuales requieren de un enfoque meticuloso en la recopilación y organización de datos.

El derecho comparado implica un minucioso análisis de las normas jurídicas, legislación y jurisprudencia de diversos países o regiones con el propósito de identificar similitudes, diferencias y patrones comunes en sus sistemas legales, específicamente en relación con el acceso no autorizado a sistemas informáticos.

El fichaje se erige como una herramienta crucial en esta investigación, pues permite ordenar y sistematizar la amplia información obtenida. Cada ficha contiene detalles específicos sobre las disposiciones legales, precedentes judiciales, doctrina y otros elementos relevantes de los sistemas jurídicos estudiados. Estas fichas actúan como una valiosa herramienta de referencia rápida y organizada, facilitando al investigador el acceso ágil a la información clave necesaria para realizar comparaciones y análisis posteriores.

Asimismo, el fichaje es fundamental para el logro de los objetivos propuestos en esta investigación. Al permitir una estructuración efectiva de los datos, facilita la identificación de patrones y tendencias relevantes en los sistemas jurídicos estudiados. Además, contribuye a la fundamentación sólida de las conclusiones y hallazgos obtenidos, lo que aporta mayor credibilidad y rigor al estudio.

En resumen, el fichaje se convierte en un aliado indispensable en esta investigación de derecho comparado, al facilitar el análisis detallado de los sistemas legales estudiados y respaldar la consecución de los objetivos propuestos. Su implementación garantiza la sistematización y organización óptimas de la información, proporcionando una base sólida para el estudio comparativo y el logro de resultados concluyentes y valiosos en el ámbito del acceso no autorizado a sistemas informáticos.

Instrumento de investigación

En este estudio de investigación, que adopta un enfoque cualitativo, se busca definir la información recopilada mediante un análisis detallado fundamentado en la base teórica establecida. Para alcanzar este objetivo, se emplea una técnica documental respaldada por citas, lo que enriquece el análisis y fortalece la redacción del trabajo. Con este propósito, se recurre a fuentes bibliográficas y otros instrumentos para llevar a cabo esta tarea de manera efectiva.

TABLA 2: Instrumentos y técnicas de investigación

Técnicas	Instrumental
Análisis del contenido	Normativa de la legislación de los países mencionados
Análisis bibliográfico	Bibliografías de autores referentes al tema a tratar
Documental	Citas

Elaborado Por: Villacreses Suarez Kevin Geovanny (2023).

3.3 **Tratamiento de la información**

La recopilación de información se llevó a cabo mediante diversas técnicas metodológicas de investigación, que incluyeron tanto citas bibliográficas como fichas correspondientes. Además, se realizaron indagaciones en documentos doctrinarios, científicos y diccionarios disponibles en la biblioteca virtual de la Universidad Estatal Península de Santa Elena. También se consultaron diversos textos y artículos en la web.

El estudio se inició con una revisión exhaustiva de las disposiciones legales de Ecuador, Perú y Venezuela con respecto a las sanciones en estos países. Esta revisión sirvió como preámbulo para comprender las sanciones relacionadas con el acceso no autorizado a los sistemas informáticos. Se destacó como un punto de observación relevante el hecho de que, a diferencia de Perú y Venezuela, Ecuador no cuenta con un código especializado exclusivamente en delitos informáticos.

En este contexto, se analizaron distintos enfoques doctrinarios, puntos de vista y teorías de diversos autores, obtenidos de diferentes artículos, libros y revistas. Estas fuentes contribuirán a una comprensión más profunda del tema investigado, centrándose en la pregunta de si la ausencia de un reglamento dedicado exclusivamente a los delitos informáticos en Ecuador afecta de alguna manera. Además, se busca corroborar o refutar la idea planteada respecto a este tema.

La revisión de los diversos artículos relacionados con la normativa ecuatoriana, peruana y venezolana reveló similitudes en los artículos de las normativas de cada país. Sin embargo, se observó que Ecuador carece de un elemento presente en los otros países en cuanto a la sanción aplicada por el delito de acceso no autorizado a los sistemas informático

3.4 Operacionalización de variables

TABLA 3: Operacionalización de variables

Variable	Conceptualización	Dimensiones	Indicaciones	Ítems	Instrumento
Sanción al tipo penal acceso no consentido de los sistemas informáticos	El acceso no consentido a sistemas informáticos es un tipo penal que se refiere a la acción de ingresar a sistemas informáticos o redes informáticas sin la debida autorización o consentimiento del propietario o administrador. Esta actividad suele estar relacionada con la violación de la seguridad de sistemas informáticos con el fin de obtener información confidencial, dañar o alterar datos, realizar actividades ilegales o cometer actos delictivos en línea. La legislación específica que regula este tipo de conducta puede variar de un país a otro, pero	Aspectos informáticos	- Recursos y Tecnología	¿Cuál es la disponibilidad de recursos financieros para investigaciones de ciberdelitos? ¿Cuán relevante es contar con los medios tecnológicos necesarios para garantizar la efectividad de la sanción?	Ficha Bibliográfica
		Aspectos sociales	- Conocimiento de la ciudadanía sobre los delitos informáticos - Desconocimiento de la sociedad sobre los ciberdelitos.	¿Cuál es la importancia del conocimiento de los ciudadanos en los delitos informáticos como el acceso no consentido a sistemas informáticos y como esto podría prevenir el aumento de este tipo de delitos? ¿Cuáles son las consecuencias del desconocimiento social en relación a la sanción establecida por el tipo penal acceso no consentido a los sistemas informáticos?	Ficha Bibliográfica
		Retos y Desafíos Futuros	- Considerar los diferentes retos que se generaran con los diferentes avances tecnológicos	¿Cómo puede llegar a afectar el desarrollo de nuevas tecnologías al cumplimiento y sanción en el tipo penal a tratar?	Ficha Bibliográfica
		Instrumento normativo	- Normativas referentes al acceso no consentido a los sistemas informáticos	¿Cuáles son los desafíos comunes que enfrentan Ecuador, Perú y Venezuela en términos de sancionar el acceso no consentido a los delitos informáticos?	Ficha Bibliográfica

	generalmente impone sanciones legales para quienes cometen este tipo de delitos, ya que comprometen la privacidad y la integridad de los sistemas y datos informáticos.			**¿**Cuáles son las sanciones o penalizaciones establecidas por la ley para aquellos que accedan ilegalmente a un sistema informático?	
		Educación y Conciencia	- Enseñanza sobre la sanción que tiene el acceso no consentido a los sistemas informáticos en los países mencionados	¿Cuán importante es el papel que tiene la sociedad y el conocimiento de la misma sobre el acceso no consentido a sistemas informáticos para evitar que el crecimiento en el índice de este tipo penal?	Ficha Bibliográfica

Elaborado por: Villacreses Suarez Kevin Geovanny (2023).

CAPÍTULO IV: RESULTADOS Y DISCUSIÓN

4.1 análisis, interpretación y discusión de resultados.

TABLA 4 Cuadro comparativo

Criterio	Ecuador	Perú	Venezuela	Coincidencias/ Semejanzas	Diferencias
Denominación del tipo penal	Acceso no consentido a un sistema informático	Acceso no consentido a un sistema informático	Acceso no consentido a un sistema informático	- Ecuador, Venezuela y Perú buscan brindar seguridad en al acceso en los respectivos sistemas informáticos	- La sanción establecida por parte de Venezuela Y Perú es levemente más fuerte en comparación con la de Ecuador.
Normativas correspondientes	Código orgánico integral penal	Ley de delitos informáticos	Ley especial contra los delitos informáticos	- Se puede evidenciar por parte de la legislación ecuatoriana, Peruana y Venezolana que en la sanción que todos estos países aplican para el tipo penal de acceso no consentido a sistemas informáticos es muy similar en cuanto a pena privativa de libertad, lo cual evidencia la importancia que estos países le dan al cometimiento y por consecuente la	- Una de las principales y más notables diferencias está en el que tanto Venezuela como Perú tienen el delito de acceso no consentido a un sistema informático dentro de un código especializado y único para los diferentes delitos informáticos que se pueden cometer, mientras que Ecuador carece de este tipo de código siendo que encontramos tipificado el acceso no consentido a un sistema informático

				sanción de este tipo de delitos informáticos. - Ecuador y Venezuela coinciden en establecer como tiempo máximo de sanción privativa de libertad la cantidad de 5 años. - Tanto la normativa de Ecuador, Perú y Venezuela suelen incluir definiciones similares respecto al acceso no consentido a un sistema informático, lo cual contribuye enormemente a la implementación de un marco legal para abordar de mejor manera el problema. - Las 3 normativa para analizar establecen artículos con enfoque en el tema estudiado, es decir el acceso no consentido a sistemas informáticos, cada una estableciendo tanto las características y la sanción para el incumplimiento la normativa.	dentro del Código Orgánico Integral Penal. - A pesar de que las normativas de los 3 países establen sanciones con pena privativa de libertad estas se diferencian en el tiempo siendo que las penas y multas varían en cada país. Ecuador impone penas de 3 a 5 años, Perú de 1 a 4 años, y Venezuela de 1 a 5 años. - En cuanto a las diferencias mas notables que encontramos en las penas está el hecho de que tanto Venezuela como Perú establecen adicional a la sanción privativa de libertad una sanción económica la cual varia levemente entre Perú y Venezuela mientras que por el lado de Ecuador este no aplica ningún tipo de sanción económica en la sanción del tipo penal estudiado. - Ecuador tiene disposiciones específicas sobre la explotación ilegítima del acceso a sistemas, como la modificación

					de sitios web o la prestación no autorizada de servicios. - Tanto en la normativa peruana como en la venezolana, no se detallan sanciones específicas para la explotación ilegítima del acceso a sistemas informáticos. En Perú, la normativa se centra en el acceso ilícito y el exceder la autorización, mientras que en Venezuela se enfoca en el acceso indebido a sistemas de tecnologías de información, sin abordar sanciones concretas para actividades posteriores de explotación ilegítima. Esta carencia de disposiciones específicas podría dar lugar a interpretaciones diversas y desafíos en la aplicación de la ley, lo que requerirá evaluaciones caso por caso en situaciones de explotación ilegítima.
Fecha de vigencia de la	10/09/2014		30/10/2001		

norma		22/10/2013			
Verbo Reactor	"Acceder". Específicamente, se prohíbe el "acceso sin autorización" a sistemas informáticos.	"Acceder" de manera "deliberada e ilegítima", siempre que se realice con la "vulneración de medidas de seguridad establecidas para impedirlo"	"Acceder" sin la debida autorización o excediendo la que hubiere obtenido		
Sujeto Activo	La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema.	El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo	Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información.		
Sujeto Pasivo	Quien tenga el legítimo derecho sobre dicho sistema	El propietario o responsable del sistema informático que está siendo objeto de acceso ilegítimo	El titular del sistema que utiliza tecnologías de información.		
Consecuencia Jurídica	Por acceder sin autorización a un sistema informático, telemático o de telecomunicaciones, o mantenerse dentro del mismo en contra de la voluntad del legítimo titular, es una pena privativa de libertad de	Por acceder deliberada e ilegítimamente a un sistema informático, siempre que se realice con vulneración de medidas de	Dicha consecuencia por acceder sin la debida autorización o excediendo la que hubiere obtenido a un sistema que		

	tres a cinco años. Si el acceso ilícito se realiza con el propósito de explotar ilegítimamente el acceso, modificar un portal web, desviar o redireccionar el tráfico de datos o voz, o prestar servicios sin autorización, la pena privativa de libertad también es de tres a cinco años.	seguridad establecidas para impedirlo, es una pena privativa de libertad no menor de uno ni mayor de cuatro años y una multa de treinta a noventa días. Esta misma pena se aplica si se accede al sistema informático excediendo lo autorizado.	utiliza tecnologías de información es una pena de prisión de uno a cinco años y una multa de diez a cincuenta unidades tributarias.		

Elaborado Por: Villacreses Suarez Kevin Geovanny (2023).

Semejanzas en el acceso no consentido a los sistemas informáticos

Es innegable que los tres dominios jurídicos de Ecuador, Perú y Venezuela, exhiben un carácter intrínseco y una estructura jerárquica que los reviste de la capacidad de salvaguardar contra el acceso no autorizado a sistemas informáticos. Sin embargo, presentan similitudes que permiten su análisis y comparación, entre las cuales cabe destacar las siguientes

- Se puede constatar a través de la legislación de Ecuador, Perú y Venezuela que la sanción impuesta en todos estos estados respecto al delito de acceso no autorizado a sistemas informáticos es notablemente similar en términos de la pena privativa de libertad. Esta similitud evidencia la relevancia que estos países otorgan a la comisión y, en consecuencia, a la sanción de este tipo de infracciones informáticas.
- La regulación en Ecuador, Perú y Venezuela a menudo incorpora definiciones parecidas en lo que respecta al acceso no autorizado a sistemas informáticos, lo que conlleva en gran medida a la establecimiento de un marco jurídico que permite abordar de manera más efectiva este problema.
- Las regulaciones en Ecuador, Perú y Venezuela hacen referencia al empleo de sistemas informáticos y tecnologías de la información como el ámbito de aplicación del delito. Esto evidencia que están formuladas con el propósito de resguardar la seguridad de la información y la integridad de los sistemas en el entorno digital.

Diferencias en el acceso no consentido a los sistemas informaticos

Asimismo, debido a las particularidades inherentes a cada contexto nacional y las necesidades artísticas presentes en los tres países bajo análisis, se observan discrepancias sustanciales que establecen una clara demarcación entre las regulaciones de Ecuador, Venezuela y Perú en lo que concierne al acceso no consentido a sistemas informáticos. A continuación, se exponen algunas de las diferencias relevantes

- En lo que respecta a las diferencias más destacadas que se pueden identificar en las sanciones, se observa que tanto Venezuela como Perú, además de imponer una pena privativa de libertad, establecen una sanción económica, la cual presenta diferencias leves entre Perú y Venezuela. En contraste, en el caso de Ecuador, no se contempla la imposición de ninguna sanción económica en relación al tipo penal objeto de estudio.

- Ecuador cuenta con disposiciones específicas en lo que respecta a la explotación ilícita del acceso a sistemas, abarcando aspectos tales como la alteración de sitios web o la provisión no autorizada de servicios.
- En la normativa peruana y venezolana, no se contemplan sanciones específicas para la explotación ilícita del acceso a sistemas informáticos. En el caso de Perú, la legislación se centra en el acceso no autorizado y en la superación de los límites de la autorización, mientras que en Venezuela, se enfoca en el acceso indebido a sistemas de tecnologías de la información, sin proporcionar sanciones concretas para las actividades subsiguientes de explotación ilícita. Esta carencia de disposiciones específicas puede dar lugar a diversas interpretaciones y desafíos en la aplicación de la ley, lo que requerirá evaluaciones caso por caso en situaciones de explotación ilícita.

4.2 Verificación de la idea a defender

En la presente investigación, en el capítulo dos, se declaró como parte de la idea a defender el que la sanción que Ecuador tiene respecto al tipo penal a estudiar era poco eficaces en comparación con la de Perú y Venezuela y luego de llevar a cabo un minucioso análisis del marco legal vigente en Ecuador, Venezuela y Perú, en lo que concierne a las regulaciones relativas al acceso no autorizado a sistemas informáticos, así como de la exhaustiva revisión de la literatura pertinente, se ha podido establecer que la sanción aplicada por Ecuador en relación al acceso no autorizado a sistemas informáticos resulta ligeramente menos efectiva en comparación con las sanciones impuestas por Perú y Venezuela para el mismo delito. Esto se debe a que la legislación ecuatoriana carece de una sanción económica adicional a la pena privativa de libertad como parte de las consecuencias jurídicas por la comisión de dicho delito, lo que la coloca en una posición de menor contundencia punitiva en relación con Perú y Venezuela.

En lo que respecta a la normativa peruana, es relevante destacar un aspecto importante, a saber, que este país establece un período de pena privativa de libertad máximo menor en comparación con Ecuador y Venezuela, limitándolo a un máximo de 4 años, mientras que los otros dos países establecen un tope de 5 años. No obstante, se destaca que la legislación peruana incluye una sanción económica equivalente a un máximo de 90 días de multa, lo que añade un componente adicional a su régimen sancionatorio.

Por otro lado, es necesario reconocer que la legislación ecuatoriana, a pesar de no contar con un código especializado en la sanción y tratamiento exclusivo de delitos informáticos, como sí lo hacen Venezuela y Perú, ni de incluir alguna forma de responsabilidad económica como parte de la sanción por la comisión del delito estudiado, tipifica de manera más detallada las conductas que se producen después de obtener acceso al sistema informático. Esto simplifica significativamente el trabajo de investigación y, de igual manera, la aplicación de la ley, al reducir el tiempo requerido para evaluar cada caso, dado que las diferentes situaciones que podrían surgir ya están previstas en la normativa.

Es entonces que los resultados de esta investigación mediante el análisis comparativo directo de las normas realizado en el capítulo 4 arrojan luz sobre la eficacia de las sanciones legales relacionadas con el acceso no autorizado a sistemas informáticos en Ecuador en comparación con las regulaciones vigentes en Perú y Venezuela. La legislación ecuatoriana se queda rezagada en términos de contundencia punitiva debido a la ausencia de una sanción económica adicional a la pena privativa de libertad, a diferencia de Perú, que impone una multa como complemento a la pena, y Venezuela, que establece tanto penas de prisión como multas.

En última instancia, estos hallazgos resaltan la necesidad de revisar y actualizar la legislación ecuatoriana en lo que respecta a los delitos informáticos, considerando la incorporación de sanciones económicas proporcionales a la gravedad de las infracciones. Este ajuste legal podría fortalecer la posición de Ecuador en la lucha contra el acceso no autorizado a sistemas informáticos y asegurar una respuesta más efectiva en la protección de la ciberseguridad en el país.

CONCLUSIONES

- La comparación exhaustiva de las sanciones legales relacionadas con el acceso no autorizado a sistemas informáticos en Ecuador, Perú y Venezuela revela que la legislación ecuatoriana carece de una sanción económica adicional a la pena privativa de libertad, lo que la coloca en una posición de menor contundencia punitiva en relación con sus homólogos.
- A través de un análisis comparativo de la legislación Ecuatoriana, Peruana y Venezolana en relación con el acceso no autorizado a sistemas informáticos, se ha observado que Ecuador presenta una regulación detallada que tipifica diversas conductas, esta claridad en la legislación podría facilitar la interpretación y aplicación de la ley en casos de delitos informáticos.
- Mientras que la legislación Ecuatoriana se distingue por su énfasis en la descripción detallada de los delitos informáticos, la legislación Peruana y Venezolana cuentan con sanciones económicas adicionales a las penas privativas de libertad lo cual favorece al poder punitivo de las mismas.
- La revisión y actualización de la legislación ecuatoriana en materia de delitos informáticos es esencial para mantenerse alineada con los avances tecnológicos y las mejores prácticas internacionales en la lucha contra el cibercrimen. Esto no solo debe contemplar la posibilidad de incorporar sanciones económicas, sino también mejoras en la capacidad de investigación y persecución de estos delitos.

RECOMENDACIONES

- Considerando la falta de una sanción económica en la legislación ecuatoriana relacionada con el acceso no autorizado a sistemas informáticos, se sugiere explorar la posibilidad de introducir medidas económicas proporcionales a la gravedad de los delitos informáticos sin necesidad de modificar la ley de manera sustancial. Esto podría fortalecer la efectividad de las sanciones legales y la disuasión de posibles infractores, contribuyendo así a una mayor protección de la ciberseguridad en el país.
- Dado que la legislación ecuatoriana es detallada en la descripción de conductas relacionadas con delitos informáticos, se recomienda enfocarse en la mejora de su claridad y accesibilidad. Esto facilitaría su comprensión y aplicación por parte de los profesionales del derecho y las autoridades.
- En virtud del exhaustivo detalle presente en la tipificación de conductas relacionadas con delitos informáticos en la legislación ecuatoriana, se plantea la necesidad imperativa de optimizar al máximo este recurso. En consecuencia, se insta a promover activamente programas de formación altamente especializados dirigidos a profesionales del derecho, jueces y fuerzas de seguridad encargados de la aplicación de la ley en el ámbito de la ciberseguridad.
- Es crucial instar que la legislación ecuatoriana se mantenga vigilante ante las evoluciones tecnológicas y la amenaza constante de delitos informáticos. Se insta a que se establezca un mecanismo constante de revisión y adaptación de la normativa en este ámbito, garantizando su flexibilidad y capacidad para enfrentar futuros desafíos cibernéticos. De esta manera, se asegurará que Ecuador continúe protegiendo efectivamente sus sistemas informáticos y luchando contra el cibercrimen en un entorno tecnológico en constante cambio.

BIBLIOGRAFÍA

Aguilar, P. A. (2015). ¿Derecho Informático ó Informática Jurídica?. *Revista de Investigación en Tecnologías de la Información, 3*(6), p. 19-24.

Benkler, Y. (2006). La Riqueza de las Redes. Icaria Editorial.

Cabanellas, T. G. (2006). *Diccionario jurídico elemental.*

Cáceres, R. S. (2018). APUNTES INTRODUCTORIOS AL DERECHO COMPARADO. *THĒMIS-Revista de Derecho* , pág. 62. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj_7-nSjqmCAxUSSzABHW6qA1kQFnoECCIQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F7049692.pdf&usg=AOvVaw1Pk26e1k-G_a88Wcs8kIdV&opi=89978449

Chavez, J. (s.f.). *Centro Europeo De postgrado.* Obtenido de CEUPE: https://www.ceupe.com/blog/sistema-informatico.html#:~:text=Definición%20de%20sistema%20informático,software%20(todo%20lo%20intangible).

Código Orgánico Integral Penal [COIP]. Art. 234. 10 de febrero de 2014 (Ecuador).

Colina, C. (2023). Manipulación algorítmica y sesgo psicosocial en redes sociales. *Temas De Comunicación*, (46), p. 6–26. Recuperado a partir de https://revistasenlinea.saber.ucab.edu.ve/index.php/temas/article/view/6219.

Comparador LegalTech . (s.f.). *Comparador LegalTech* . Obtenido de https://www.comparador-legaltech.com/herramientas/jurimetria/#:~:text=Jurimetría%20es%20una%20herramienta%20de,de%20millones%20de%20decisiones%20judiciales.

Del Pino, S. A., & Martín, S. (2008). Delitos informáticos: generalidades. *Recuperado el 15 de junio de 2023 de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf*.

Editorial Etecé. (5 de agosto de 2021). *https://concepto.de/teoria-de-sistemas/*. Obtenido de https://concepto.de/teoria-de-sistemas/

Fernández, M., & Hassan Montero, Y. (16 de febrero de 2003). *No Solo Usabilidad*. Obtenido de https://www.nosolousabilidad.com/articulos/ai.htm

Génova, M. & Guzmán, J. (1983). Teoría de Sistemas. Universidad Nacional Abierta.

Gonzáles, J., Bermeo, J., Villacreses, E. & Guerrero, J. (2018) Delitos Informáticos: Una revisión sistemática. *Conference Procedings UTMACH, 2*(1). p. 178-190.

Latour, B. (2008). Reensamblar lo social: Una introducción a la teoría del actor-red. Manantial.

Lessig, L. (2001). El Código y otras leyes del ciberespacio. Taurus Digital.

Lessig, L. (2009). El código 2.0. Traficantes de sueños.

Ley de Delitos Informáticos [LDI]. Art. 2. 22 de octubre de 2013 (Perú).

Loevinger, L. (1948). Jurimetrics: The Next Step Forward. *Minnesota Law Review*, *33*(5), p. 405-408.

María, M. C. (2013). *Universidad de Castilla*. Obtenido de revista en cultura de la legalidad: http://hdl.handle.net/10578/4431

Pino, D. S. (2016). Delitos Informáticos: Generalidades. Ecuador: Pontificia Universidad Católica del Ecuador. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Rodríguez, A. (1990). Análisis de la Ley de Fraude Informático. *Revista de Derecho de UNAM, 192(5)*.

Téllez, J. (2009). *Derecho Informático* (4ta Edición). McGraw Hill.

Teoría jurídica y "derecho comparado". Una aproximación y un deslinde (2007) Rolando Tamayo y Salmorán

Methods of Comparative Law por Geoffrey Samuel (2012)

Derecho Comparado y Globalización Jurídica de Manuel Cepeda Espinosa y José María Serna de la Garza (2005)

Derecho Comparado: Historia, metodología y problemas de René David y John E.C. Brierley (1984)

Derecho Comparado: Texto y materiales de Esin Örücü y David Nelken (1995)

Diccionario de Ciencias Jurídicas, Políticas y Sociales de Manuel Ossorio (2011)

Diccionario de Términos Jurídicos de Enrique Alcaraz Varó y Brian Hughes(2007)

ANEXOS

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD CARRERA DE DERECHO

ANEXO 1: GUÍA DE COMPARACIÓN NORMATIVA DE LOS PAÍSES DE ECUADOR, PERU Y VENEZUELA EN CUANTO AL ACCESO NO AUTORIZADO A SISTEMAS INFORMATICOS

Criterio	**País**	**país**	**país**	**Coincidencias/ Semejanzas**	**Diferencias**
Denominación del tipo penal					.
Normativas correspondientes				.	
Fecha de vigencia de la norma					
Verbo Reactor	.				
Sujeto Activo					
Sujeto Pasivo			.		
Consecuencia Jurídica		.	.		

ANEXO 2: GUIA DE TABLA DE OPERACIÓN DE VARIABLES

Variable	Conceptualización	Dimensiones	Indicaciones	Ítems	Instrumento