UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

Opción de Titulación:

Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo

Tema:

ANÁLISIS COMPARATIVO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DEL ECUADOR CON LA LEGISLACIÓN CHILENA DESDE UN ENFOQUE DE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

Autor:

Damián Marcelo Gutiérrez Meneses

Director:

Miguel Arturo Arcos Argudo

Cuenca – Ecuador
2024

Autor:

Damián Marcelo Gutiérrez Meneses
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
gutierrezmdamian@gmail.com

Dirigido por:

Miguel Arturo Arcos Argudo
Magister en Seguridad de las Tecnologías de la Información y de las Comunicaciones.
Doctor en Ciencias de la Computación para Smart Cities.
marcos@ups.edu.ec

DEDICATORIA

Este logro tan significativo está dedicado especialmente a ti, mi pequeña princesa CarlitaLu. Gracias por iluminar mi vida y ser mi fuente inagotable de motivación día tras día.

AGRADECIMIENTO

A mi esposa Jessy, quien siempre ha estado a mi lado con un apoyo inquebrantable en todo momento. Y a mi querida CarlitaLu, mi fuente constante de motivación y alegría.

Tabla de Contenido

ANÁLISIS COMPARATIVO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DEL ECUADOR CON LA LEGISLACIÓN CHILENA DESDE UN ENFOQUE DE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

Autor:

DAMIÁN MARCELO GUTIÉRREZ MENESES

Resumen

Este documento presenta un análisis comparativo de las leyes de protección de datos personales en Chile y Ecuador con un enfoque en la ciberseguridad y los delitos informáticos. La protección de la información personal ha emergido como una prioridad esencial en este contexto. El estudio se llevó a cabo considerando los marcos legales, regulatorios y normativos de ambos países.

El análisis se enfoca en elementos fundamentales relacionados con los principios de protección de datos personales. Además, explora cómo las leyes abordan la prevención y sanción de delitos informáticos, tales como la violación de datos personales, el acceso y recepción no autorizados, así como el fraude y la falsificación informática. Este análisis profundiza en las similitudes y diferencias entre los marcos legales de ciberseguridad y delitos informáticos en Chile y Ecuador, resaltando las fortalezas y limitaciones de cada país.

Finalmente ofrece recomendaciones para fortalecer la protección de datos personales al momento que se desee implementar un SGSI, adaptando controles efectivos para salvaguardar la privacidad ciudadana y prevenir amenazas cibernéticas.

Palabras clave:

Protección de datos personales, SGSI, LOPDP, delitos informáticos, ley orgánica, análisis comparativo.

ABSTRACT

This document presents a comparative analysis of personal data protection laws in Chile and Ecuador with a focus on cybersecurity and computer crimes. The protection of personal information has emerged as an essential priority in this context. The study was carried out considering the legal, regulatory and normative frameworks of both countries.

The analysis focuses on fundamental elements related to the principles of personal data protection. In addition, it explores how laws address the prevention and punishment of computer crimes, such as the violation of personal data, unauthorized access and receipt, as well as computer fraud and forgery. This analysis delves into the similarities and differences between the legal frameworks of cybersecurity and computer crimes in Chile and Ecuador, highlighting the strengths and limitations of each country.

Finally, it offers recommendations to strengthen the protection of personal data when implementing an ISMS, adapting effective controls to save citizen privacy and prevent cyber threats.

Keywords:

Personal data protection, SGSI, LOPDP, cybercrime, organic law, comparative analysis.

1. Introducción

La imparable incorporación de las tecnologías de la información ha suscitado una creciente preocupación por la seguridad en el ciberespacio, llevando a los países a adoptar marcos regulatorios eficaces para hacer frente a estos desafíos en constante evolución. En este contexto, la protección de los datos personales se erige como un pilar fundamental para salvaguardar la privacidad y seguridad de las personas.

Tanto Chile como Ecuador han respondido a esta imperante necesidad promulgando leyes específicas en materia de protección de datos personales y delitos informáticos. Estas legislaciones no solo buscan garantizar asegurar la protección de la información confidencial, sino también establecer medidas eficaces para prevenir y sancionar a los delincuentes informáticos que puedan comprometer la privacidad de los ciudadanos.

El enfoque de esta investigación se centra en un análisis comparativo entre la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador y la legislación chilena, con especial atención a los aspectos relacionados con ciberseguridad y delitos informáticos. La comprensión de estas normativas es fundamental no solo para el cumplimiento legal, sino también para fortalecer la capacidad de los países en la prevención y respuesta efectiva frente a amenazas digitales.

A lo largo de esta exploración, se analiza inicialmente la parte conceptual necesaria para comprender las similitudes, diferencias y áreas de mejora en ambos marcos legales. Además, se desarrolla recomendaciones que contribuyan al fortalecimiento de la seguridad y al cumplimiento de los requisitos normativos de un Sistema de Gestión de Seguridad de la Información (SGSI).

2. Determinación del Problema

En la actualidad, gracias a las tecnologías y conexiones disponibles, es posible transmitir datos personales a cualquier parte del mundo en cuestión de segundos. Sin embargo, esta facilidad no está exenta de desafíos, debido a que, al dispersar información en diversos puntos de la red, se crea una identidad digital que puede revelar aspectos de la vida privada de una persona, como sus gustos, identidad, actividades, y mucho más. Esto resalta la creciente importancia de cumplir con las regulaciones de protección de datos personales, las cuales son fundamentales para mantener un adecuado control sobre esta información.

Con los rápidos avances tecnológicos y la continua globalización, desde finales del siglo XIX hasta la actualidad, resulta esencial ajustarnos presurosamente a las transformaciones disruptivas que exigen. Cada vez es más común el intento de vulnerar la privacidad de los datos personales o su uso indebido, debido a la inmensa cantidad de información que generamos diariamente, lo que plantea un riesgo significativo para la seguridad y la integridad de estos datos.

En el contexto previamente mencionado, surge la necesidad de salvaguardar la privacidad de los datos personales y, de alguna manera, evitar la identificación en internet. Como se expone en el artículo "La protección de datos", esta necesidad conduce a la urgencia de regular el derecho a la protección de datos como un derecho autónomo y tipificar las leyes de delitos informáticos [1]. Es esencial contar con marcos legales que salvaguarden los datos personales, y en Ecuador, esto se consigue mediante la LOPDP, respaldada por las sanciones penales estipuladas en el Código Orgánico Integral Penal (COIP).

3. Reseña histórica de la protección de datos personales

El artículo "Declaración Universal de los Derechos Humanos" señala que ya a finales del siglo XIX existían indicios de la protección de la privacidad de la vida. Un siglo después, el 10 de diciembre de 1948, en París, se estableció el reglamento contenido en la Declaración Universal de los Derechos Humanos, la cual fue acogida y aceptada por la Asamblea General de las Naciones Unidas. Esta declaración, disponible para su revisión en la Resolución 217A-(III), establece las bases relacionadas con las leyes de derechos humanos y la vida privada [2]. Con el avance de la informática y las telecomunicaciones en los años siguientes, surgieron leyes jurídicas a nivel nacional y supranacional. Estas leyes fueron diseñadas con el propósito de garantizar la efectiva aplicación de los derechos mencionados, especialmente en lo que respecta a la seguridad y privacidad de la información en este contexto tecnológico en constante evolución [3].

En cuanto a la preocupación por la protección de datos personales, en Europa, a finales de la década de los años 70, se estableció la primera ley relacionada con la protección de datos personales. Países como Alemania y España lo hicieron en el año 1977; seguidos por Dinamarca, Francia y Austria en 1978, y Luxemburgo en 1979. En mayo de 2018, la Unión Europea (UE) consolidó el Reglamento General de Protección de Datos (“GDPR”). Este reglamento establece normas para la gestión de datos personales y se convirtió en una guía esencial en materia de protección de datos para varios países [4].

El artículo "Redes sociales y polarización. Cuando el algoritmo amplifica las emociones humanas" destaca que la implementación del Reglamento General de Protección de Datos generó reformas en la legislación de protección de datos personales en varios países latinoamericanos [5]. Por ejemplo, Chile promulgó una ley integral en 1999, Paraguay en 2000, Uruguay en 2008, Argentina en 2000,

Panamá en 2002, Brasil en 1997 y Ecuador en 2021, con un período de adaptación de dos años para su aplicación [6].

3.1 ¿Qué es una ley orgánica?

Existen dos tipos de leyes vigentes en Ecuador: leyes orgánicas y leyes ordinarias; la diferencia radica principalmente en la materia de acción ante órganos jurisdiccionales y en el porcentaje de votos para la aprobación o negación. Es decir, las leyes orgánicas pueden ser aprobadas con un porcentaje mayor al 75% de los votos de la Asamblea, mientras que las leyes ordinarias bastan con la mitad más uno para poder aprobarse. Las leyes orgánicas prevalecen sobre las leyes ordinarias [7].

La Asamblea Nacional en Ecuador es la entidad responsable de aprobar las leyes; antes de obtener la categoría de ley, un proyecto debe ser presentado y respaldado ante el presidente de dicha Asamblea. Este proceso puede ser llevado a cabo por el presidente de la República, los Asambleístas con al menos el 5% de sus integrantes, la Corte Constitucional, la Procuraduría General del Estado, la Defensoría del Pueblo, así como por ciudadanos y organizaciones sociales que cuenten con al menos el 0,25% de los inscritos en el patrón electoral nacional [8].

Según la “Reforma de la Constitución de la República del Ecuador”, modificado el 25 de enero de 2021, en el artículo 133, indica textualmente los requisitos para que sean consideradas como leyes orgánicas y ordinarias [9]. Se expone textualmente:

1. Las que regulen la organización y funcionamiento de las instituciones creadas por la Constitución.
2. Las que regulen el ejercicio de los derechos y garantías constitucionales.
3. Las que regulen la organización, competencias, facultades y funcionamiento de los gobiernos autónomos descentralizados.
4. Las relativas al régimen de partidos políticos y al sistema electoral.

3.2 Importancia de implementar una ley de protección de datos personales

El artículo “Protección de datos: sus orígenes y la privacidad desde el diseño” resalta que este tipo de normas precautelan “la protección de la dignidad humana, la preocupación jurídica por la intimidad y el resultado del impacto social que ha sido el resultado desde la aparición de los ordenadores” [10].

La posesión y uso de los datos personales suponen una ventaja estratégica y competitiva para las empresas. El artículo “La evolución de las estrategias de marketing en el entorno digital: implicaciones jurídicas” hace relación que “al sacar partido a la información puede suponer la clave para crear y desarrollar estrategias exitosas para cualquier negocio. Los datos o bases de datos son herramientas de trabajo capaces de proporcionar información sobre una actuación concreta en la población como un todo, ofreciéndonos una estimación de las tendencias recientes y los riesgos de futuro a escala nacional” [11]. Hoy en día varias empresas invierten grandes cantidades de dinero en publicidad y marketing con objetivos netamente comerciales: conseguir más visibilidad en su entorno, prevalecer entre la competencia, aumentar sus ventas y tomar decisiones críticas para mantearse dentro del mercado [12].

Expresiones como "cuando el producto es gratis, el producto eres tú" o "usted no solo está siendo observado, usted está siendo vendido" subrayan la conexión con la recopilación de datos personales por parte de terceros en diversas situaciones donde los usuarios acceden a servicios gratuitos, como al navegar por páginas web, registrarse en redes sociales, descargar aplicaciones móviles o utilizar buscadores online [13]. Aunque los usuarios no pagan directamente por estos servicios, terceras personas obtienen sus datos personales, adquiriendo así información esencial sobre gustos, pensamientos y deseos.

Entre las principales maneras en las que se ha visto vulnerada la privacidad de los datos personales está el recibir constantes llamadas, sin consentimiento, de

operadoras de telefonía móvil, ofertas de crédito o adquisición de tarjetas bancarias, sin haber autorizado el uso de dicha información lo que se puede deducir que son obtenidos mediante venta ilegal o filtración de datos personales.

Estos datos son obtenidos, almacenados y posteriormente compartidos o vendidos por terceros cuando, por ejemplo, se realiza la apertura de una cuenta bancaria, al llenar formularios de supuestos descuentos en tiendas de distintos productos de consumo, al adquirir un plan celular con una determinada empresa de telefonía, al llenar fichas médicas en instituciones de salud, al crear una cuenta en redes sociales, entre otros más [14].

La información que obtienen terceros no siempre es usada de manera adecuada, al tener datos críticos como nombres completos, números de cédula o pasaporte, direcciones de correo electrónico, fechas de nacimiento, profesión de la persona, entre otros, puede ser mal usado mediante conductas discriminatorias o con fines delictivos como estafas y extorsiones.

3.3 Ley de protección de datos personales en Chile

La Constitución Política de Chile, a través de la Ley 19628, garantiza la protección y el respeto de los datos personales de los ciudadanos. Publicada el 28 de agosto de 1999, esta normativa busca regular el tratamiento y la salvaguarda de datos personales en el ámbito del Derecho Civil [15]. Es importante destacar que esta ley no se aplica al emitir opiniones o con fines informativos, especialmente cuando estas actividades son realizadas por medios de comunicación. A lo largo del tiempo, se ha actualizado para adaptarse a los diversos cambios tecnológicos, como las redes sociales, el comercio electrónico y las ciberamenazas, entre otros [16].

La ley chilena establece diversos derechos para las personas cuyos datos son tratados por terceros. Entre estos derechos se encuentran el acceso a la información sobre el origen, finalidad y destinatarios de sus datos, así como detalles sobre el tratamiento recibido. Además, se concede el derecho a rectificar datos

inexactos o incompletos, la supresión de datos cuando ya no son necesarios o se ha revocado el consentimiento, la limitación de tratamiento a finalidades específicas, la portabilidad de los datos en un formato estructurado, y la oposición al tratamiento, con excepciones para intereses legítimos o necesidades de defensa en reclamaciones. Estos derechos forman parte de un marco legal destinado a proteger la privacidad y el control de la información personal de los individuos.

3.4 Ley de protección de datos personales en Ecuador

Según antecedentes, en Ecuador, la Ley Orgánica de Protección de Datos Personales tuvo su origen como proyecto el 19 de septiembre de 2019, impulsada por la iniciativa del expresidente Lenin Moreno. Este impulso fue motivado por una seria filtración de datos personales en el país, resultado de fallos informáticos que afectaron a diversos funcionarios del Gobierno de ese entonces. Conforme a un informe de la empresa israelí de seguridad vpnMentor, la filtración se originó desde un servidor en Miami, EE. UU., gestionado por la empresa ecuatoriana Novaestrat, especializada en publicidad. La filtración, que abarcó 18 gigabytes, incluyó información personal como nombres, números de teléfono y datos educativos, laborales y financieros [17]. Expertos como Noam Rotem y Ran Locar destacaron que esta violación de datos implicó una gran cantidad de información sensible a nivel individual [18].

El 10 de mayo de 2021, la LOPDP fue aprobada por la Asamblea Nacional y, tras debates subsiguientes, fue promulgada por el expresidente de la República. Según el artículo "Aprobación de la Ley Orgánica de Protección de Datos Personales", esta legislación se ajusta a estándares internacionales, situando a Ecuador como un país con un nivel adecuado para el manejo de datos sin dificultades significativas [19]. A partir de esa fecha, las empresas contaron con dos años para adaptarse a los procesos y normativas establecidas por la ley.

Iniciado en octubre de 2017, el proceso legislativo contempló una fase de adaptación para empresas, tanto públicas como privadas [20], la cual entró en vigor el 22 de mayo de 2023. Su objetivo primordial es posibilitar que las empresas trabajen con datos personales de manera informada y segura, resguardando la privacidad y asegurando un uso adecuado de la información.

3.4.1 Principios y derechos de la Ley Orgánica de Protección de Datos Personales en Ecuador

La LOPDP en Ecuador establece un marco integral que regula el tratamiento de datos personales, sustentado en principios y derechos fundamentales. El objetivo principal es garantizar el pleno ejercicio del derecho a la privacidad y la preservación de la información personal de los ciudadanos [21]. A continuación, se proporciona una descripción de cada uno de los principios y derechos establecidos por esta legislación:

TABLA 1 PRINCIPIOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DE ECUADOR

Juridicidad	El tratamiento de datos debe cumplir las leyes de la Constitución
Lealtad	El tratamiento de datos debe ser claro y transparente para el titular en cuanto a su tratamiento
Transparencia	La información sobre el tratamiento de datos debe ser accesible y comprensible
Finalidad	Los datos sólo pueden usarse para los fines específicos informados
Pertinencia y minimización	Los datos deben ser adecuados, relevantes y limitados a lo necesario
Proporcionalidad	El tratamiento debe ser apropiado y no excesivo
Confidencialidad	Se debe guardar secreto y no revelar los datos indebidamente
Calidad y exactitud	Los datos deben ser exactos y debidamente actualizados
Conservación	Los datos se deben mantener sólo el tiempo necesario para cumplir la finalidad
Seguridad	Se deben tomar medidas técnicas y organizativas para proteger los datos
Responsabilidad	El responsable debe demostrar la aplicación de medios de protección y que cumple con las obligaciones legales
Aplicación favorable del titular	En caso de dudas aplicables se debe favorecer los derechos del titular de datos personales
Independencia del control	El control sobre la protección de datos debe ser autónomo e imparcial

TABLA 2 DERECHOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DE ECUADOR

Información	Derecho a que se informe de manera completa sobre el tratamiento de los datos personales
Acceso	Derecho a acceder y conocer a detalle los datos personales que el responsable de tratamiento mantiene
Rectificación y actualización	Derecho a corregir datos inexactos o incompletos
Eliminación	Derecho al borrado de los datos personales en ciertos casos de inconsistencias por parte del responsable de tratamiento
Oposición	Derecho a oponerse a determinados tratamientos
Portabilidad	Derecho a recibir los datos de manera íntegra y en formato electrónico o transferirlos a otro responsable de tratamiento
Suspensión de tratamiento	Derecho a suspender el tratamiento en ciertos supuestos
No automatización	Derecho a no estar sujeto a decisiones automatizadas
Consulta	Derecho a la consulta pública y gratuita de registros ante el Registro Nacional de Protección de Datos Personales
Educación digital	Derecho a capacitación sobre protección de datos personales

4. Marco teórico referencial

Cuando se habla de los derechos que tienen las personas en cuanto a la protección de datos, se hace referencia a la obligación que tiene el Estado de garantizar seguridad jurídica y el consentimiento en cuanto a la búsqueda, obtención, acceso, almacenamiento y procesamiento de datos personales, ya sea por parte de una organización pública o privada. El ciudadano tiene derecho a conocer en todo momento quien dispone de esta información, la manera en la que se la utiliza, así como oponerse a la tenencia y utilización [22].

El artículo "La doble clasificación del expediente clínico, analizada desde el contenido de la Ley General de Protección Datos Personales del Derecho a la Información" [23] indica que los datos personales son "cualquier información concerniente a una persona física, identificada o identificable". En otras palabras, se refiere a la información que pertenece directamente a una persona, por ejemplo: los nombres, número de cédula de identidad o cualquier dato que podría identificarla, por ejemplo: correo electrónico o su número de teléfono.

La protección de datos personales se convierte en un derecho cuando existe una ley que lo respalda. La información que generamos cuando usamos la tecnología como medio de consulta, tiene un valor económico para muchas de las empresas y puede exponernos como consumidores al conocer nuestras referencias para ofrecernos publicidad adaptada a nuestros gustos y necesidades [24], por ejemplo, la preferencia política de una persona es información de gran interés para una empresa que se dedica a llevar a cabo campañas políticas, ya sea para respaldar sus puntos de vista o incluso intentar influir en ellos a través de la publicidad.

Por citar unos casos notables de filtración de información, se destaca el incidente de Equifax en 2017; esta agencia de crédito líder en Estados Unidos experimentó una violación de datos que afectó a más de 143 millones de personas, comprometiendo información vital como nombres, direcciones, números de

teléfono, números de seguro social y detalles de tarjetas de crédito [25]. Además, en 2018, la cadena hotelera Marriott International, una de las más grandes del mundo, sufrió una filtración de datos que impactó a más de 5 millones de clientes. La información comprometida incluyó nombres, direcciones, números de teléfono, datos de tarjetas de crédito y detalles de reservas [26]. Estas filtraciones evidencian un impacto significativo en las personas afectadas, exponiéndolas a un mayor riesgo de fraude y robo de identidad. Subrayan la imperiosa necesidad de contar con leyes robustas de protección de datos personales para salvaguardar la privacidad de las personas.

4.1 Sistema de Gestión de Seguridad de la Información (SGSI)

Según la norma internacional ISO/IEC 27001:2013 se entiende por un SGSI a un "enfoque sistemático usado para gestionar, establecer, implementar, monitorear, mantener y mejorar un conjunto de procesos referente al contexto de Seguridad de la Información de un todo o parte de una organización de cualquier tamaño. El objetivo primordial que busca el SGSI es el de gestionar eficientemente la accesibilidad de la información y ayudar a cumplir objetivos comerciales" [27].

El artículo "Análisis e implementación para la integración del sistema de Información (SGSI) ISO 27001 con aplicación Uranium Backup para protección de servidores virtuales en plataforma VMWARE ESXI, replicación y recuperación en la empresa Comercial e Industrial Sucre COMSUCRE S.A." [28] indica que un SGSI es una herramienta usada como una guía de buenas prácticas para establecer directrices, procedimientos y políticas necesarias para garantizar la vital triada de la información: confidencialidad, integridad y disponibilidad (CID), en lo que respecta a los activos de información de una organización. De esta forma, se busca evaluar y reducir al mínimo los riesgos latentes que puedan amenazar la seguridad de la información. Resulta fundamental comprender los conceptos fundamentales que sustentan sus tres pilares principales:

1. Confidencialidad: Implica que únicamente el personal autorizado tendrá acceso a los datos o información.
2. Integridad: Se refiere al estado de los datos o información y garantiza que no puedan ser modificados de forma deliberada o accidental en ningún caso.
3. Disponibilidad: Significa que los datos, la información o los servicios deben estar accesibles en cualquier momento en que se requieran.

Es importante considerar una ley de protección de datos personales cuando se desea implementar un SGSI porque esta ley establece los lineamientos que se deben cumplir para para garantizar que la información de las personas se trate de manera segura y confidencial.

4.2 Definición de Hacker

Explorando la historia del término "hacker", en 1959, estudiantes del Instituto de Tecnología de Massachusetts fueron pioneros al utilizar las primeras computadoras TX-0 para una amplia variedad de actividades, que abarcaron desde proyectos de investigación, programación y resolución de problemas, hasta experimentación y simulación. Sus logros fueron tan significativos que incluso los creadores de las computadoras no habían imaginado todas las posibilidades que podrían lograrse con ellas. A finales de los años 80 y 90, con la llegada de las computadoras de escritorio y por medios de comunicación e investigación, el término de hacker se mal relacionó con otro que se refería al de un “pirata informático“ debido a que en esas épocas existían demostraciones en cuanto a la tecnología y juegos de computadora donde grupos llamados “crackers” utilizaban métodos para burlar seguridades en los juegos y poder revenderlos a precios más económicos. Los “crackers”, del vocablo inglés “crack” (que significa romper), es un término aplicado a la persona que intenta descubrir información de carácter sensible usando técnicas para romper las seguridades de un sistema informático sin permiso alguno y muchas de las veces con intenciones de obtener algún beneficio propio [29].

El artículo “La ética del hacker y el espíritu de la era de la información” indica que “un hacker es una persona que no necesariamente debe tener un perfil informático,

que se encarga de encontrar errores de seguridad en una red de equipos computarizados" [30].

El artículo de "Tipos de Hackers" resalta que un hacker es una persona con gran conocimiento en informática o telecomunicaciones que domina y se mantiene capacitado en lenguajes de programación y con altas posibilidades de burlar las seguridades informáticas para acceder a información sensible [31].

En este contexto, se pueden explorar dos perspectivas complementarias de la terminología "hacker". Desde un punto de vista ético, un hacker, sin importar su perfil profesional, se dedica a identificar y corregir vulnerabilidades en sistemas informáticos para mejorar la seguridad sin incurrir en prácticas delictivas. Mientras que, desde la perspectiva maliciosa, este hacker usa sus habilidades técnicas con el objetivo de explotar vulnerabilidades con intenciones como el robo de información, causar daños o la ejecución de fraudes,

4.3 Hacker Ético

El artículo titulado como "Hacker ético vs. delincuente informático" [32] indica que un hacker ético es un profesional que posee conocimiento en el área de informática, que, en un ambiente controlado, realiza algún tipo de ataque a una red de computadores para conocer el actual nivel de seguridad aplicado y encontrar posibles vulnerabilidades que puede tener un sistema informático. Estas actividades las realiza de manera planificada y con una previa autorización del dueño del sistema.

El artículo "Formación de Auditores Internos ISO27001 y Técnicas de Hacking ético" [33] expone que un hacker ético es la persona que usa sus conocimientos de seguridad informática para defender los sistemas informáticos contra amenazas existentes en el ciberespacio. Es quien analiza el origen de las amenazas, aplica controles con el objetivo primordial de eliminarlas. Además, es el encargado de buscar vulnerabilidades en las redes informáticas para posteriormente reportarlo y

sugerir que se realicen las respectivas correcciones, esto sin hacer ningún tipo de daño.

Los dos autores previamente mencionados coinciden en sus conceptos acerca del perfil profesional y las responsabilidades de un hacker ético. Estos individuos no se involucran en actividades maliciosas, ya que su labor se centra en tareas autorizadas destinadas exclusivamente a reforzar la seguridad de los sistemas informáticos dentro de una organización. Utilizando técnicas de monitoreo y eliminación de amenazas, su objetivo es prevenir o al menos reducir al mínimo los posibles ataques informáticos. Su motivación no es el lucro, sino que, por el contrario, reciben una compensación por descubrir vulnerabilidades, las cuales posteriormente informarán a los encargados de la seguridad informática.

4.4 Delitos informáticos

Un delito informático puede describirse como “un conjunto de conductas criminales que se realizan a través del ordenador para obtener información de manera ilícita o que afectan al funcionamiento de los sistemas informáticos” [34]. Este término no ha sido definitivo ya que ha ido mejorando con el pasar del tiempo y con los cambios tecnológicos que han surgido de la evolución de las Tecnologías de Información y Comunicación y las propias conductas delictivas en la sociedad.

La historia de los delitos informáticos se remonta a décadas atrás, y un claro ejemplo es el virus Melissa, reconocido como uno de los más agresivos en 1999. Es un malware, elaborado por David L. Smith, se diseñó para propagarse masivamente a través de correos electrónicos usando las 50 primeras direcciones de correo en el sistema afectado. Smith difundió un archivo llamado "list.doc" en una comunidad online, indicando que contenía contraseñas para acceder a contenido adulto. Su objetivo era alterar registros de Windows, replicarse por correo y dañar varios tipos de archivos en las computadoras de las víctimas. El impacto fue tan devastador que empresas como Microsoft, Intel y AOL bloquearon sus conexiones para evitar su propagación. Los daños estimados ascendieron a unos 80 millones de dólares,

mayormente afectando a empresas estadounidenses. El creador fue enjuiciado y condenado a 20 meses de prisión por este delito informático [35].

El artículo titulado "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad" proporciona una perspectiva general sobre los delitos y el terrorismo en el ciberespacio desde la aparición de los sistemas informáticos y la red mundial (internet). Expone que los ciberdelincuentes han buscado constantemente formas de vulnerar los sistemas informáticos, empleando técnicas avanzadas para eludir las medidas de seguridad implementadas por las empresas. Entonces, hoy en día, existe un nuevo y evolutivo espacio donde delincuentes aprovechan situaciones o vulnerabilidades informáticas para cometer actos delictivos mediante ciberataques. En respuesta a esta amenaza, propone la identificación de los tipos de delitos y la aplicación de sanciones cuando se violan las leyes. Además, destaca la importancia de un monitoreo constante de las amenazas, dada la frecuente evolución tecnológica, para anticiparse a la delincuencia [36]. El artículo subraya que combatir la ciberdelincuencia va más allá de tener un sistema defensivo o utilizar tecnologías de última generación; es necesario trabajar con un enfoque integral de defensa como medida de protección para preservar la integridad humana, social y económica de una nación.

El artículo "Análisis conceptual del delito informático en Ecuador" atribuye el aumento de los delitos informáticos a la constante evolución de las tecnologías de información y al crecimiento del mercado negro de la información. Destaca los cambios significativos en la normativa legal ecuatoriana, especialmente con la introducción de la Ley de Comercio Electrónico y la promulgación del Código Orgánico Integral Penal en 2014. Sin embargo, señala que las leyes actuales sobre delitos informáticos en Ecuador son demasiado generales y sugiere la necesidad de una especificación para cada tipo de delito, con el objetivo de brindar una mayor seguridad a posibles víctimas [37].

El artículo titulado "Los Ciberdelitos y su tipificación en el Código Orgánico Integral Penal (COIP)" realiza un análisis de las leyes destinadas a asegurar la protección contra ciberdelitos. Este análisis se respalda en materiales investigativos y

encuestas realizadas a profesionales del área penal. El artículo destaca la necesidad de medios informáticos y tecnológicos, así como la falta de conocimiento en las víctimas, como elementos clave para la perpetración de delitos informáticos. Concluye destacando que la falta de información entre los ciudadanos es el factor determinante en la comisión de estos delitos. En este sentido, se propone la implementación de políticas preventivas y un plan integral de capacitación y divulgación por parte de las entidades gubernamentales, abordando aspectos doctrinarios de los delitos informáticos como una solución para concientizar a la población sobre la naturaleza y prevención de estos actos [38].

4.4.1 Ejemplos de delitos informáticos

El artículo "Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC" sostiene que la seguridad de la información es una de las principales preocupaciones de los directivos de empresas. Esta inquietud resulta comprensible al considerar la cantidad de noticias que circulan en los medios acerca de robos o hackeos a sistemas empresariales, muchos de los cuales involucran información confidencial [39].

Al examinar las estadísticas nacionales de ciberseguridad, resulta evidente que Ecuador no está exento de sufrir ataques informáticos que comprometen la integridad de los datos y la confidencialidad de la información. Según un informe de la Fiscalía General del Estado, las denuncias por delitos informáticos en nuestro país han experimentado un inquietante aumento en los últimos cinco años, tanto en frecuencia como en gravedad e impacto, lo que hace que los métodos de prevención y detección sean cada vez menos eficaces. A medida que el tiempo avanza, los ciberataques se vuelven más frecuentes y los niveles de seguridad implementados inicialmente en las organizaciones tienden a debilitarse. Este escenario ha llevado a muchas instituciones a adoptar medidas de prevención y control más rigurosas para salvaguardar tanto los datos como la infraestructura.

De acuerdo con la mundialmente conocida Compañía Kaspersky, el Ecuador se encuentra dentro de la lista de países que presenta más ataques informáticos. De hecho, en el 2014, el Ecuador se colocó en el octavo puesto entre los países Latinoamericanos [40]. Por otra parte, según una investigación del Diario NotiPress, el Ecuador se encuentra en el puesto 98 de 193 países en riesgos de ciberseguridad según el Índice Global de Ciberseguridad. Entre las principales ciberamenazas que se han detectado están: la suplantación de identidad, malware y ataques phishing [41].

La publicación del periódico "Luz de América" hace relación al más grande ciberataque realizado a la institución financiera más grande de Ecuador en una conocida institución financiera y ocurrido a inicios del mes de octubre de 2021. El banco cuenta con aproximadamente 1,5 millones de clientes y un capital de 1500 millones de dólares. Se realizaron múltiples quejas a la institución por varios de los clientes al sentir intermitencia y no poder usar de manera normal los servicios ofrecidos por el banco a través de canales electrónicos. Un accionista de la organización indicó "la institución está siendo víctima de un incidente de ciberseguridad contra los sistemas informáticos por lo que nos hemos visto obligados a inhabilitar parcialmente los servicios, sin embargo, este incidente no afecta su desempeño financiero "[42]. Las medidas iniciales que habría tomado el banco es la de aislar parte de la red comprometida de la parte principal de la red bancaria para evitar propagación y mayor afección. También realizar una profunda investigación forense y una auditoría interna sobre los hechos ocurridos con profesionales en el área de ciberseguridad. Mediante un informe entregado posteriormente por el banco a la Superintendencia de Bancos indicaron que los ataques de ciberseguridad fueron realizados por expertos informáticos y conocidos a nivel internacional y que el banco si cuenta con infraestructura adecuada estandarizada en cuanto a seguridad informática [43]. Según un historial, este tipo de problemas que ha presentado la institución no es el primero. En el mes de febrero 2021 existió un comunicado en su cuanta oficial de twitter donde indicaban que muchos datos de usuarios de clientes de tarjetas de crédito fueron

comprometidos “Conocemos que hubo un acceso no autorizado a los sistemas de un proveedor que presta servicios de mercadeo”.

De la misma manera, la Corporación Nacional de Telecomunicaciones del Ecuador (CNT) fue víctima de un delito informático el 14 de julio del 2021 donde mediante un ciberataque dejó indispuesto a varios de sus sistemas como, por ejemplo, el servicio de pagos en línea por medio de facturación y canales de atención al cliente [44]. El Diario Primicias en su artículo “Los misterios del ataque que dejó a CNT sumida en la “emergencia”” indica: “que la Corporación Nacional de Telecomunicaciones asume que el ataque que sufrieron fue muy fuerte, pero no se comprometió información sensible ni tampoco se entregó dinero para rescatarla” [45]. Dicho ataque que se definió como un Ransom de tipo EXX (conocido por deteriorar las configuraciones de seguridad de un sistema informático para que quede vulnerable a cualquier tipo de ataque de malware, generalmente cifrado de datos) que desestabilizó el correcto funcionamiento de sus sistemas por más de una semana, pero posteriormente fue controlado, descartando un posible contagio en otras instituciones del estado. En este ataque también se habló de que se tuvo acceso a los sistemas de la Corporación mediante un ataque de phishing en el que los ciberdelincuentes utilizaron el correo electrónico para robar datos de uno o varios usuarios de la institución. Posteriormente CNT expuso la respectiva denuncia formal ante la Fiscalía de Ecuador por delito de “ataque al sistema informático” para poder recabar información sobre el hecho ocurrido [46] pero hasta el momento no se han dado a conocer detalles específicos del ciberataque, ni la magnitud ni las intenciones reales del mismo.

5. Materiales y metodología

A continuación, se detalla la metodología empleada para realizar el análisis comparativo de la legislación sobre delitos informáticos y ciberseguridad, con un enfoque en la protección de datos personales de los ciudadanos. La metodología propuesta abarca los siguientes pasos:

1. Revisión bibliográfica: Revisión documental relacionada con las leyes de Chile y Ecuador misma que establece una base informativa para el posterior análisis.
2. Organización de Componentes: Los componentes de las leyes se estructuran en una agrupación paralela. Esta estructura organizativa permite una comparación más efectiva y un análisis más claro de los aspectos normativos de ambos países.
3. Análisis comparativo: Mediante la investigación y comparación de las leyes de ambos países.
4. Exploración de alcance y enfoque: Examinando el alcance y analizando la manera en la que las leyes abordan aspectos de delitos informáticos.
5. Conclusiones y recomendaciones: En base al análisis realizado donde se redactan conclusiones de forma estructurada y se formulan recomendaciones específicas.

5.1 Comparación de delitos informáticos según las leyes de protección de datos de Chile y Ecuador

Se realiza una comparativa entre las disposiciones legales relacionadas con los delitos informáticos y ciberseguridad en Chile y Ecuador. Es imperioso indicar que, en Chile, el marco legal aplicable es el Código Penal, mientras que en Ecuador se rige por el Código Orgánico Integral Penal. Estos códigos detallan las normativas y sanciones pertinentes para diversos tipos de delitos en cada país. La comparativa

comienza con la presentación de cuadros que resalta las similitudes normativas, seguida de un análisis comparativo para examinar las diferencias y similitudes entre ambas jurisdicciones.

TABLA 3 NORMATIVA PENAL ENTRE ART.1 DE CHILE Y ART. 232 DE ECUADOR

Chile	***Artículo 1: Ataque a la integridad de un sistema informático*.** El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.
	Sanción: Presidio menor en su grado medio a máximo. (541 días a 5 años).
Ecuador	***Artículo 232: Ataque a la integridad de sistemas informáticos.*** **a.** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático. Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo. **b.** Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana.
	Sanciones: **a.** Pena privativa de libertad de 3 a 5 años. **b.** Pena será de 5 a 7 años de privación de libertad.

Al analizar las similitudes entre los artículos detallados en la Tabla 3 con respecto a la integridad de los sistemas informáticos, tanto Chile como Ecuador han establecido disposiciones legales específicas, aunque con enfoques y matices particulares. En el ámbito del alcance, Chile se centra en el ataque a la integridad de un sistema informático, obstaculizando su funcionamiento mediante la introducción, transmisión, daño, deterioro, alteración o supresión de datos. Por otro lado, en Ecuador, el delito abarca la destrucción, daño, borrado, alteración, suspensión, mal funcionamiento o comportamiento de sistemas informáticos, dispositivos electrónicos o infraestructura tecnológica. Además, se penaliza la creación y distribución de dispositivos maliciosos. En cuanto a las acciones consideradas delito, ambos países coinciden en sancionar la obstaculización del funcionamiento normal de los sistemas informáticos y la introducción de elementos maliciosos. En términos de gravedad, mientras que en Chile no se especifica, en

Ecuador se considera más grave si afecta bienes informáticos vinculados con servicios públicos o la seguridad ciudadana. En el enfoque de protección, la legislación chilena se centra en salvaguardar la integridad de los sistemas informáticos y su funcionamiento, especialmente frente a la manipulación de datos. Por su parte, la ley ecuatoriana tiene un enfoque más amplio, protegiendo la infraestructura tecnológica y buscando sancionar cualquier acción que cause daño, alteración o mal funcionamiento de los sistemas.

TABLA 4 NORMATIVA PENAL ENTRE ART. 2 Y 6 DE CHILE Y ART. 234 DE ECUADOR

Chile	***Artículo 2: Acceso ilícito*.** **a.** El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático. **b**. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. **c.** En caso de ser una misma persona la que hubiere obtenido y divulgado la información.
	Sanciones: **a.** Presidio menor en su grado mínimo o multas de 11 a 20 Unidades Tributarias Mensuales. **b**. Presidio menor en sus grados mínimo a medio. **c.** Presidio menor en sus grados medio a máximo.
	***Artículo 6: Receptación de datos informáticos*.** El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°.
	Sanción: Pena asignada a los respectivos delitos, rebajada en un grado.
Ecuador	***Artículo 234: Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.*** **a.** 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. **b.** 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.
	Sanciones: **a**. Pena privativa de la libertad de 3 a 5 años, **b.** Pena privativa de la libertad de 3 a 5 años.

Al analizar las similitudes entre los artículos detallados en la Tabla 4, los cuales se enfocan al acceso ilícito a sistemas informáticos, tanto Chile como Ecuador han establecido marcos legales específicos con algunos matices notables. En cuanto al alcance, Chile se centra en el acceso ilícito, ya sea sin autorización o excediendo la

autorización existente, mientras que Ecuador amplía el concepto incluyendo sistemas telemáticos y de telecomunicaciones. Ambos países consideran delito el acceso sin autorización y el mantenimiento no consentido en el sistema. En cuanto a la acción delictiva, Chile penaliza el acceso ilícito con el propósito de apoderarse o utilizar la información, así como la divulgación de información obtenida ilegalmente. En Ecuador, además de considerar delito el acceso no consentido, se sanciona la explotación ilegítima del acceso, la modificación de portales web y otras acciones específicas. Respecto al acceso, Chile penaliza tanto el acceso sin autorización como el acceso que excede la autorización y busca apoderarse o utilizar la información. Ecuador considera delito el acceso no consentido sin importar la intención, pero especifica acciones adicionales que también constituyen delito. En términos de protección, ambas legislaciones buscan salvaguardar la seguridad e integridad de los sistemas informáticos, pero mientras Chile se enfoca en sancionar el acceso ilícito y la divulgación de información obtenida de manera ilegal, Ecuador amplía su enfoque a la protección de sistemas telemáticos y de telecomunicaciones, sancionando el acceso no consentido y la explotación ilegítima de los sistemas y servicios.

TABLA 5 NORMATIVA PENAL ENTRE ART. 3 Y 8 DE CHILE Y ART. 230 DE ECUADOR

Chile	***Artículo 3: Interceptación ilícita*.** **a.** El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos **b.** El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos.
	Sanciones: **a.** Presidio menor en su grado medio **b.** Presidio menor en sus grados medio a máximo.
	***Artículo 8: Abuso de los dispositivos*.** El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos.
	Sanción: Presidio menor en su grado mínimo y multa de 5 a 10 UTM.

Ecuador	***Artículo 230: Interceptación ilegal de datos.*** **a.** La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. **b.** La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder. **c.** La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior. **d.** La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. **e.** La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.
	Sanción: Pena privativa de libertad de 3 a 5 años.

Al examinar las similitudes presentes en la Tabla 5 con relación a delitos informáticos, se constata que Chile y Ecuador han instaurado marcos legales con enfoques específicos. En términos de alcance, ambos países penalizan la interceptación ilegal de información en sistemas informáticos. En Chile, el artículo 3 de la ley se centra en la interferencia y captación no autorizada de datos, mientras que, en Ecuador, el artículo 230 aborda la interceptación ilegal y acciones asociadas como el diseño o envío ilegítimo de contenido digital. Las acciones consideradas delito incluyen la interceptación y acciones relacionadas en ambos países, pero con énfasis en diferentes aspectos técnicos. La intención y consecuencias de estas leyes también difieren: en Chile, se busca penalizar la interceptación ilícita y abuso de dispositivos con consecuencias sujetas al sistema judicial, mientras que, en Ecuador, el objetivo es prevenir y sancionar estos delitos, con consecuencias establecidas legalmente. En cuanto al enfoque de protección, ambas leyes buscan resguardar la seguridad de los sistemas informáticos y la privacidad de la información, imponiendo sanciones a aquellos que realicen acciones ilícitas.

TABLA 6 NORMATIVA PENAL ENTRE ART. 4 DE CHILE Y ART. 195 DE ECUADOR

Chile	***Artículo 4: Ataque a la integridad de los datos informáticos.*** El que indebidamente altere, dañe o suprima datos informáticos, y siempre que cause un daño grave al titular.
	Sanción: Presidio menor en su grado medio.
Ecuador	***Artículo 195: Infraestructura ilícita.*** La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.
	Sanción: Pena privativa de libertad de 1 a 3 años.

Al analizar los artículos detallados en la Tabla, se revelan enfoques divergentes entre Chile y Ecuador. En Chile, el delito se centra en el ataque a la integridad de los datos informáticos, requiriendo que la alteración, daño o supresión cause un daño grave al titular para ser considerado delito. La ley chilena se orienta a proteger la integridad de los datos y los derechos de los titulares, sancionando las acciones que afecten estos datos. En cambio, en Ecuador, el delito está vinculado a la posesión de infraestructura, programas, equipos, bases de datos o etiquetas que permitan modificar la información de identificación de un equipo terminal móvil. La gravedad requerida para considerar el delito no está especificada, y la apertura de bandas para la operación de equipos terminales móviles no se considera delito. La ley ecuatoriana se enfoca en la protección de la identificación de los equipos terminales móviles, buscando sancionar la posesión de elementos que posibiliten modificar esa información.

TABLA 7 NORMATIVA PENAL ENTRE ART. 5 DE CHILE Y ART. 234,1 DE ECUADOR

Chile	***Artículo 5: Falsificación informática*.** **a.** El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos. **b.** Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio.
	Sanciones: **a.** Presidio menor en sus grados medio a máximo **b.** Presidio menor en su grado máximo a presidio mayor en su grado mínimo

Ecuador	***Artículo 234,1: Falsificación informática.*** **a.** La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos. **b.** Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1.
	Sanciones: **a.** Pena privativa de libertad de 3 a 5 años **b.** Sancionado con la misma pena.

La Tabla 7 proporciona un análisis destacando diferencias significativas. En Chile, el delito se centra en la adulteración informática, abarcando acciones como la introducción, alteración, daño o supresión indebida de datos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos. La ley chilena especifica que, si esta conducta es realizada por un empleado público abusando de su oficio, se considera un delito de mayor gravedad. Por otro lado, en Ecuador, el delito se refiere a la falsificación informática con la intención de provocar un engaño en las relaciones jurídicas. Se considera delito la introducción, modificación, eliminación o supresión de contenido digital con la intención de producir datos o documentos falsos. Además, se penaliza el uso de documentos producidos a partir de contenido digital que haya sido objeto de los actos ilícitos mencionados. Mientras que la ley chilena se centra en proteger la autenticidad de los datos y la integridad de los documentos, la ley ecuatoriana busca resguardar la veracidad de la información y la confianza en las relaciones jurídicas.

TABLA 8 NORMATIVA PENAL ENTRE ART. 7 DE CHILE Y ART. 190 DE ECUADOR

Chile	***Artículo 7: Fraude informático.*** **a, b, c.** El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático. Se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.

	Sanciones: **a.** Presidio menor en sus grados medio a máximo y multa de 11 a 15 UTM, si el valor del perjuicio excediera de 40 UTM. **b.** Presidio menor en su grado medio y multa de 6 a 10 UTM, si el valor del perjuicio excediere de 4 unidades tributarias mensuales y no pasare de 40 UTM. **c.** Presidio menor en su grado mínimo y multa de 5 a 10 UTM, si el valor del perjuicio no excediere de 4 UTM. Si el valor del perjuicio excediere de 400 UTM, se aplicará la pena de presidio menor en su grado máximo y multa de 20 a 30 UTM
Ecuador	***Artículo 190: Apropiación fraudulenta por medios electrónicos.*** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.
	Sanción: Pena privativa de libertad de 1 a 3 años.

Al analizar las similitudes entre los artículos detallados en la Tabla 8, se evidencia que las legislaciones de Chile y Ecuador abordan el fraude informático con enfoques distintos. En Chile, el delito se centra en el fraude informático, definido como la manipulación de un sistema informático con la finalidad de obtener beneficio económico. La ley chilena penaliza la introducción, alteración, daño o supresión de datos informáticos, así como cualquier interferencia que cause perjuicio a otra persona. Además, se considera autor a aquel que facilite los medios para cometer el delito, aun cuando desconozca su ilicitud. Por otro lado, en Ecuador, el delito se refiere a la apropiación fraudulenta por medios electrónicos, penalizando el uso fraudulento de sistemas informáticos y redes electrónicas con la intención de apoderarse de bienes ajenos o transferir bienes, valores o derechos sin consentimiento. La ley ecuatoriana aborda métodos específicos, como la alteración, manipulación o modificación del funcionamiento de diversas tecnologías. Mientras que la ley chilena se centra en proteger la integridad y el funcionamiento correcto de los sistemas informáticos y prevenir fraudes económicos, la ley ecuatoriana tiene un enfoque más amplio al proteger los bienes, valores y derechos de las personas y

garantizar la seguridad de los sistemas informáticos y redes electrónicas frente a actividades fraudulentas.

5.2 Resultados del análisis comparativo en las leyes de protección de datos personales de Chile y Ecuador

Se presentan los resultados más significativos obtenidos del análisis comparativo de las leyes de protección de datos personales en Chile y Ecuador. El propósito es identificar distintos criterios enfocados en similitudes, diferencias, enfoques y desafíos clave presentes entre los dos marcos normativos en lo que respecta a la recolección, procesamiento, almacenamiento y transferencia de datos personales:

1. Ambos países han promulgado leyes específicas para proteger los datos personales, reconociendo la importancia de preservar la privacidad de los ciudadanos.
2. Las leyes de ambos países incorporan principios y conceptos fundamentales de pautas internacionales, como el reglamento general de protección de datos (RGPD) de la Unión Europea.
3. En ambas jurisdicciones, es esencial obtener el consentimiento explícito del titular para el tratamiento de datos personales.
4. Chile y Ecuador otorgan al titular de datos el derecho de acceder, rectificar, conocer, oponerse, controlar y eliminar la información personal.
5. Ambos países imponen restricciones sobre la comercialización, cesión o transferencia de estos datos sin consentimiento del titular de datos personales.
6. En ambos países, el responsable de tratamiento de datos está obligado a mantener en secreto los datos personales, especialmente cuando provienen de fuentes no accesibles al público.
7. Ambas leyes establecen sanciones para los responsables de tratamiento de datos que incumplen las disposiciones establecidas, resaltando la seriedad con la que se debe tomar la protección de datos personales.

8. Tanto en Chile como en Ecuador, se impone la responsabilidad a los organismos públicos y privados de cuidar los datos personales con diligencia.
9. En cuanto a la eliminación de datos personales, Chile y Ecuador coinciden en la necesidad de eliminar datos cuando termina el tratamiento o cuando el titular de datos ejerce su derecho de supresión.
10. En lo que respecta a los tiempos de respuesta del responsable de tratamiento ante solicitudes de los titulares de datos personales, Chile no especifica un período concreto, mientras que Ecuador destaca un plazo de quince días hábiles.
11. Ambos países resaltan la importancia de la clasificación de datos personales. Chile incorpora datos caducos y estadísticos, mientras que Ecuador incluye datos biométricos y genéticos.
12. Chile y Ecuador concuerdan en que los datos personales deben considerarse como información privada, reconociendo que su tratamiento inadecuado puede afectar la privacidad, la autonomía y la dignidad de las personas.
13. En Chile, no hay obligación legal de designar un Oficial de Datos personales (DPO), mientras que, en Ecuador, esta designación es obligatoria para instituciones públicas o empresas privadas con tratamiento de datos a gran escala.
14. En cuanto a las transferencias internacionales de datos personales, en Chile no se requiere autorización previa, mientras que en Ecuador es necesario obtener la aprobación previa de la autoridad de control antes de realizar cualquier transferencia de datos al extranjero.

6. Recomendaciones a considerar en el desarrollo de un SGSI alineado a la LOPDP

Un SGSI alineado con el cumplimiento de la protección de datos personales ayuda a consolidar la confianza al demostrar un compromiso sólido con la gestión de riesgos relacionados con la seguridad de la información. Este compromiso se vuelve fundamental en un entorno de constante evolución de amenazas cibernéticas y protección de datos personales, donde la capacidad de salvaguardar la información personal se convierte en un activo valioso tanto para la institución como para sus partes interesadas.

A continuación, se detallan una serie de recomendaciones fundamentales que deben considerarse al diseñar un SGSI alineado con la protección de datos personales, contemplando las sanciones establecidas por el COIP en relación con los delitos informáticos. Estas recomendaciones se fundamentan en las normativas vigentes tanto de Ecuador como de Chile y están diseñadas para ofrecer un valor significativo cuando se implementan de manera efectiva.

Definir las partes interesadas del SGSI. Para esto se debe considerar los puntos de vista de clientes, empleados, accionistas o propietarios, proveedores y los distintos entes regulatorios. Al conocer las necesidades de las partes interesadas, la institución debe implementar medidas de seguridad enfocadas en la LOPDP. De esta manera, permitirá mantener una gestión responsable de los datos y cumplir con las obligaciones legales.

Definir responsables de las distintas áreas dentro de la institución. En este punto se debe considerar especialmente el rol del DPO, quien será el encargado de velar por el cumplimiento de la LOPDP. Así mismo actúa como punto de contacto entre los ciudadanos y el ente regulador, garantizando el cumplimiento normativo en

materia de protección de datos personales en la institución. Su rol permite fortalecer la seguridad y privacidad de la información, asegurando un manejo responsable y adecuado de los datos sensibles.

Inventario y clasificación la información teniendo en cuenta la confidencialidad y sensibilidad. En este punto se debe crear un inventario tecnológico analizando cuidadosamente los datos que son almacenados, procesados y transmitidos para determinar su naturaleza y relevancia en términos de sensibilidad. Para ello se debe realizar una validación del contenido para determinar si existen datos personales. Con esto, se deben establecer estrategias para la aplicación de medidas de seguridad según el nivel de criticidad que ayuden a garantizar la privacidad de los datos.

Identificar los riesgos asociados con el manejo de datos personales de la institución. En consecuencia, es necesario considerar las amenazas y vulnerabilidades con probabilidad de materializarse y que puedan afectar la confidencialidad y privacidad. La gestión de riesgos es efectiva para aplicar medidas de seguridad que ayuden a mitigar los riesgos identificados y garantizar la protección adecuada de la información personal. Se puede sugerir la metodología Magerit por su adaptabilidad, enfoque en escenarios y alineación con estándares como ISO/IEC 27001 que permiten una identificación más realista y priorización de riesgos.

Comprender a detalle los controles aplicables a la seguridad de la información y a la protección de datos personales. Se debe tener en cuenta la aplicabilidad de controles eficaces relacionados a la familia ISO 27000, la LOPDP y una serie de guías de mejores prácticas. Adicional a esto, llevar a cabo el monitoreo continuo y la actualización constante de procedimientos conforme a las últimas normativas, es necesario para mantener una protección robusta y adecuada de la información.

Implementar controles de seguridad de los datos siguiendo las mejores prácticas. Como las recomendadas en la norma ISO/IEC 27002, ISO 27702 y respaldándose en marcos de referencia y técnicas que ayudan en este aspecto. La técnica de

anonimización de datos puede ser una alternativa para evitar que cierta información haga identificable a un ciudadano. Así mismo, controles como el acceso a la información, encriptación de datos sensibles, gestión de incidentes de seguridad y la concientización del personal en materia de privacidad, son fundamentales para fortalecer los temas asociados con la privacidad y confidencialidad de datos personales.

Evaluar el cumplimiento de los controles aplicados en la institución mediante planes de auditoría continuas. Esto para garantizar la efectividad de las medidas de protección implementadas y fortalecer la protección de la información sensible relacionada a la LOPDP. El objetivo de esta actividad es identificar posibles brechas que afecten a la seguridad de la información y aplicar acciones correctivas para prevenir incidentes de seguridad relacionados con la pérdida o violación de datos personales.

Definir políticas, procesos y procedimientos enfocados en salvaguardar la privacidad de los datos. Con esta actividad, se debe asegurar la manera en que la información se recopila, procesa, transmite y almacena se realice en estricto cumplimiento de las regulaciones y leyes aplicables para garantizar los derechos de los ciudadanos. Estas medidas en conjunto permiten lograr una gestión integral y segura de la información sensible, minimizando los riesgos de brechas de seguridad en cumplimiento de los estándares de privacidad requeridos.

Implementar herramientas tecnológicas como medidas de apoyo para garantizar controles efectivos. Con esto se busca mitigar potenciales riesgos asociados a ciberataques o brechas de seguridad, considerando: cifrado de archivos, firewalls, FDS, DLP, IPS, IDS y antivirus con protección avanzada. De esta manera es posible detectar comportamientos anómalos de manera proactiva y proteger los datos personales.

Aplicar una gestión de incidentes de seguridad alineada a las necesidades de la institución. Esto se logra estableciendo controles y actualización de las últimas amenazas y vulnerabilidades. Es importante establecer planes de respuesta y

contingencia que aborde de forma proactiva cualquier posible incidente de seguridad que pueda comprometer la confidencialidad de datos personales. Es necesario establecer procedimientos claros que contemplen el tratamiento de la información, cláusulas de confidencialidad y acuerdos de protección de datos con terceros para asegurar la transparencia en el manejo y protección de datos.

Aplicar mecanismos de control de acceso a la información sensible de la institución para proteger la confidencialidad y privacidad de los datos personales. Esto, mediante la aplicación de políticas que garanticen la autenticidad del personal autorizado, condiciones de acceso y la asignación de roles y transacciones específicas a los sistemas informáticos. Es importante implementar y fomentar el uso de contraseñas robustas, autenticación multifactor, limitar privilegios de acceso y establecer controles de auditoría para monitorear actividades sospechosas o inusuales.

Implementar políticas internas disciplinarias que aseguren el cumplimiento normativo del SGSI y la LOPDP. Esto se logra con el establecimiento de responsabilidades y obligaciones sobre el manejo y protección de datos personales. Es fundamental llevar a cabo capacitaciones para todos los empleados de la institución, asegurando que las políticas plenamente conocidas y comprendidas, y que brinden detalles sobre las sanciones que se aplicarán en caso de incumplimiento.

Implementar capacitaciones y simulacros que aborden la posibles incidentes de seguridad. Esto para evitar o minimizar incidentes de seguridad como fugas de información o infiltración de datos. Es necesario identificar a todos los involucrados, asignar responsabilidades claras, establecer plazos de recuperación y contar con planes de contingencia bien definidos. Estas acciones son fundamentales para reducir al mínimo el impacto de los incidentes y para asegurar una recuperación ágil y eficaz en caso de que se materialicen.

Definir procesos y procedimientos claros y coherentes que establezcan opciones de mejora continua en el SGSI. Esto se debe implementar de manera que permita

garantizar una gestión efectiva de la seguridad y la privacidad en el manejo de datos personales de la institución. Realizar evaluaciones periódicas permite identificar procesos de mejora y recomendar soluciones para fortalecer la protección de la información.

7. Conclusiones

En base al análisis comparativo de las leyes de protección de datos personales de Chile y Ecuador desde un enfoque en ciberseguridad y delitos informáticos, es importante destacar las siguientes conclusiones:

La LOPDP en Ecuador entró en vigor el 10 de mayo de 2021, mientras que, en Chile, la legislación correspondiente entró en vigor el 18 de agosto de 1999. No obstante, la ley ecuatoriana presenta una ventaja significativa al haber sido desarrollada en un contexto de creciente conciencia sobre la importancia de la protección de datos personales.

Las leyes de protección de datos personales de Chile y Ecuador coinciden en varios aspectos. Ambas garantizan a los titulares de datos derechos como el acceso, rectificación, supresión, oposición y portabilidad de sus datos. Exigen la obtención de consentimiento previo para el tratamiento de datos personales, establecen la presencia de autoridades de control, la obligación de notificar brechas de seguridad y la imposición de sanciones por incumplimiento.

La aplicación de la LOPDP en Ecuador es de gran importancia debido a la salvaguardia de la privacidad y los derechos de los ciudadanos. Esta ley cumple estándares internacionales lo que proporciona un marco legal sólido que obliga a las organizaciones públicas y privadas a proteger y gestionar de manera responsable los datos personales, garantizando su confidencialidad y privacidad. Lo que protege a los ciudadanos de posibles abusos o usos indebidos de su información.

Establecer un SGSI alineado a la ley de protección de datos personales, es fundamental para proteger la privacidad y la integridad de la información personal de los ciudadanos. Seguir estas reglas no solo significa cumplir con los requisitos legales, sino también respaldar de manera activa la seguridad de los datos, creando un entorno seguro que cumple con las leyes actuales.

El desafío para ambas legislaciones en el cumplimiento efectivo de la ley de protección de datos personales reside en lograr que se implementen de manera efectiva y se cumplan de manera rigurosa. Esto implica asegurarse de que las entidades responsables comprendan plenamente sus obligaciones y deberes, y adopten las medidas necesarias para acatar las reglas establecidas en las leyes y normativas aplicables.

Referencias

[1] Ramón Oró Badia, La protección de datos, (Barcelona: Editorial UOC, 2015), 11

[2] “Declaración Universal de los Derechos Humanos,” [En línea]. Available: https://es.wikipedia.org/wiki/Declaraci%C3%B3n_Universal_de_los_Derechos_Humanos/.[Último acceso: 8 11 2022].

[3] Tovar, V. M. C. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS: HISTORIA, FILOSOFÍA Y ALCANCE INTERNACIONAL. y Derechos Humanos, 267.

[4] Boza Díaz, L. (2017). La protección de datos personales por el Tribunal Europeo de derecho humanos y la incidencia de la tecnología en su evolución.

[5] Magallón Rosa, R., & Campos, E. (2021). Redes sociales y polarización. Cuando el algoritmo amplifica las emociones humanas.

[6] Sánchez Pérez, G., & Rojas González, I. (2012). Leyes de protección de datos personales en el mundo y la protección de datos biométricos–Parte I.

[7] “LEYES ORGÁNICAS Y ORDINARIAS,” [En línea]. Available: https://ecomundo.edu.ec/leyes-organicas-y-ordinarias/.[Último acceso: 18 11 2022].

[8] “¿Cómo se crean las leyes en el Ecuador?,” [En línea]. Available: https://www.pbplaw.com/es/infografia-como-crean-leyes-ecuador/.[Último acceso: 19 11 2022].

[9] Del Ecuador, A. C. (2008). Constitución de la República del Ecuador. Quito: Tribunal Constitucional del Ecuador. Registro oficial Nro, 449, 79-93.

[10] “Protección de datos: sus orígenes y la privacidad desde el diseño,” [En línea]. Available: https://mujeresenelsectorpublico.com/proteccion-de-datos-sus-origenes-y-la-privacidad-desde-el-diseno/.[Último acceso: 14 10 2022].

[11] Rivera Sanclemente, M. D. R. (2015). La evolución de las estrategias de marketing en el entorno digital: implicaciones jurídicas.

[12] Colin, C., & Poullet, Y. (2011). Sociedad de la información y marketing: case study. In Protección de datos personales en la sociedad de la información y la vigilancia (pp. 229-273). La Ley.

[13] Magallón Rosa, R., & Campos, E. (2021). Redes sociales y polarización. Cuando el algoritmo amplifica las emociones humanas.

[14] “Los graves riesgos de la vulneración de datos personales,” [En línea]. Available: https://www.elcomercio.com/blogs/economia-de-a-pie/graves-riesgos-vulneracion-datos-personales.html.[Último acceso: 15 11 2022].

[15] “Claves de la Ley Orgánica de Protección de Datos Personales de Chile,” [En línea]. Available: https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-chile/#:~:text=Define%20los%20principios%20para%20el,eventuales%20infracciones%20que%20pudieran%20derivarse.[Último acceso: 19 11 2022].

[16] “Protección de datos personales en Chile 2020,” [En línea]. Available: https://www2.deloitte.com/cl/es/pages/legal/articles/proteccion-datos-personales-chile.html.[Último acceso: 12 11 2022].

[17] “Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano,” [En línea]. Available: https://www.bbc.com/mundo/noticias-america-latina-49721456/.[Último acceso: 25 10 2022].

[18] Ochoa Marcillo, A. C. (2021). Desafíos globales del cibercrimen: caso Ecuador período 2014–2019 (Master's thesis, Quito, EC: Universidad Andina Simón Bolívar, Sede Ecuador).

[19] “Aprobación Ley Orgánica de Protección de Datos Personales,” [En línea]. Available: https://www.pbplaw.com/es/aprobacion-ley-organica-de-proteccion-de-datos-personales/#:~:text=El%20viernes%2C%2021%20de%20mayo,10%20de%20mayo%20de%202021./.[Último acceso: 25 10 2022].

[20] “Ley de Protección de Datos Personales,” [En línea]. Available: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/.[Último acceso: 15 11 2022].

[21] “Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador,” [En línea]. Available: https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/. [Último acceso: 24 11 2023].

[22] “La protección de datos personales de niños, niñas y adolescentes: respuestas desde el ordenamiento jurídico chileno,” [En línea]. Available: https://www.scielo.cl/scielo.php?pid=S0718-52002021000100111&script=sci_arttext#fn24/.[Último acceso: 19 11 2022].

[23] Mejía, J. A., & Morales, C. A. S. La doble clasificación del expediente clínico, analizada desde el contenido de la Ley General de Protección Datos Personales. del Derecho a la Información, 481.

[24] “¿Qué son los datos personales? ¿Cómo protegerlos?,” [En línea]. Available: https://serendipia.digital/tutoriales/que-son-los-datos-personales-como-protegerlos/.[Último acceso: 22 11 2022].

[25] “Incidente de seguridad de datos de Equifax: Lo que debe saber,” [En línea]. Available: https://consumidor.ftc.gov/alertas-para-consumidores/2019/07/incidente-de-seguridad-de-datos-de-equifax-lo-que-debe-saber.[Último acceso: 31 10 2023].

[26] “Fuga de información en la cadena hotelera Marriott,” [En línea]. Available: https://unaaldia.hispasec.com/2018/12/fuga-informacion-marriott.html.[Último acceso: 31 10 2023].

[27] “ISO27000.ES,” [En línea]. Available: https://www.iso27000.es/sgsi.html.[Último acceso: 12 11 2022].

[28] Gómez Andrade, C. A., & Doménech Álvarez, G. A. (2022). Análisis e implementación para la integración del sistema de información (SGSI) ISO 27001 con aplicación uranium backup para protección de servidores virtuales en plataforma VMWARE ESXI, replicación y recuperación en la Empresa comercial e industrial Sucre Comsucre SA (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

[29] PEREZ CRUZ, J. A. (2007). SEGURIDAD EN INTERNET.

[30] Himanen, P. (2015). La ética del hacker y el espíritu de la era de la información.

[31] Quispe, C. A. F. (2018). Tipos de Hackers.)

[32] (Gacharná, F. I. (2009). Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. Inventum, 4(6), 46-49.).

[33] Ruiz Gómez, J. C. (2018). Formación de auditores internos ISO27001 y técnicas de Hacking ético.

[34] PEREZ LUÑO, Antonio Enrique, “Manual de Informática y derecho”, Editorial Ariel, Barcelona, España, 1996, pag. 18.

[35] “En retrospectiva: el virus Melissa,” [En línea]. Available: https://www.welivesecurity.com/la-es/2016/07/19/retrospectiva-virus-melissa/. [Último acceso: 19 11 2022].

[36] Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20), 80-93.

[37] Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343-351.

[38] Castro Montoya, B. M., & Elizalde Albán, D. A. (2021). Los Ciberdelitos y su tipificación en el Código Ôrganico Integral Penal (Bachelor's thesis, Universidad de Guayaquil, Facultad de Jurisprudencia Ciencias Sociales y Polìticas).

[39] Cruz Diaz, M. A., & Fukusaki Infantas, S. (2017). Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC.

[40] “Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021,” [En línea]. Available: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/.[Último acceso: 12 12 2022].

[41] El Periodico USA. (6 de mayo de 2022). Retos y oportunidadades de la politica de ciberseguridad en Ecuador. https://www.elperiodicousa.com/retos-yoportunidades-de-la-politica-de-ciberseguridad-enecuador/#~:text=%2D%20Ecuador%20se%20encuentra%20en%20el,y%20sociedad%20civil%20estar%C3%A1n%20integradas.

[42] “El mayor banco de Ecuador sufre un ciberataque,” [En línea]. Available: https://www.primicias.ec/noticias/economia/banco-pichincha-incidente-inhabilito-servicios/.[Último acceso: 10 12 2022].

[43] “Ecuador: Ciberataque a Banco Pichincha fue de hackers internacionales,” [En línea]. Available: https://www.mascontainer.com/ecuador-ciberataque-a-banco-pichincha-fue-de-hackers-internacionales/.[Último acceso: 10 12 2022].

[44] “Ciberataque contra la operadora estatal de Ecuador, CNT EP,” [En línea]. Available: https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/ciberataque-operadora-estatal-ecuador-cnt-ep/.[Último acceso: 11 12 2022].

[45] “Los misterios del ataque que dejó a CNT sumida en la “emergencia”,” [En línea]. Available: https://www.primicias.ec/noticias/tecnologia/los-misterios-del-ataque-que-dejo-a-cnt-sumida-en-emergencia/.[Último acceso: 11 12 2022].

[46] “La Corporación Nacional de Telecomunicaciones CNT EP a la opinión pública - CNT presentó denuncia ante la Fiscalía,” [En línea]. Available: https://institucional.cnt.com.ec/noticias/la-corporacion-nacional-de-telecomunicaciones-cnt-ep-a-la-opinion-publica-cnt-presento-denuncia-ante-la-fiscalia/.[Último acceso: 11 12 2022]