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 Argentina desde un enfoque de ciberseguridad y delitos informáticos


Autores:

Cristian Javier Rubio Ganchala

Daniel Alejandro Terán Suárez

Director:

Miguel Arturo Arcos Argudo



Cuenca – Ecuador

2023

**Autores:**

**Cristian Javier Rubio Ganchala**
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
crubiog94@hotmail.com

**Daniel Alejandro Terán Suárez**
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
daniels_2408@hotmail.com

**Dirigido por:**

**Miguel Arturo Arcos Argudo**
Magíster 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


Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación Argentina desde un enfoque de ciberseguridad y delitos informáticos

***DEDICATORIA***

A Dios, por ser mi guía, mi fortaleza y mi luz en este camino de aprendizaje y crecimiento. A mi hijo, quien ha sido mi mayor motivación y quien me ha inspirado a seguir adelante en cada momento. A mi familia, por su amor incondicional, apoyo y paciencia durante todos estos años. ¡A todos aquellos que me brindaron su ayuda y apoyo, gracias de todo corazón! Este logro es también de ustedes.

Cristian Rubio

Dedico el resultado de este trabajo a mi madre y toda mi familia, que me apoyaron y contuvieron los momentos malos en la búsqueda de ser mejor persona y excelente profesional. Gracias por enseñarme a afrontar las dificultades sin perderme en el camino ni morir en el intento. Me han enseñado a ser la persona que soy hoy, mis principios, mis valores, mi perseverancia y mi empeño. Todo esto con todo el cariño del mundo y sin pedir nada a cambio.

Daniel Terán

***AGRADECIMIENTO***

En primer lugar, agradezco a mi madre que siempre me han brindado su apoyo incondicional para poder cumplir todos mis objetivos personales y académicos. A toda mi familia que con su cariño me han impulsado siempre a perseguir mis metas frente a las adversidades, haciendo que me concentre en los estudios y nunca abandonarlos".

También a mi tutor por su dedicación y paciencia, sin sus palabras y correcciones no hubiese podido lograr llegar a cumplir mi meta tan anhelada. Gracias por su guía y todos sus consejos.

A todos mis docentes, que han sido parte de mi camino universitario, y a todos ellos les quiero agradecer por transmitirme los conocimientos necesarios para poder lograr este sueño de ser un mejor profesional.

Además, a mis compañeros, los cuales muchos de ellos se han convertido en mis amigos, cómplices y hermanos. Gracias por las horas compartidas, los trabajos realizados en conjunto y las historias vividas"

Por último agradecer a la Universidad Politécnica Salesiana que me ha permitido obtener mi tan ansiado título. Agradezco a cada directivo por su trabajo y por su gestión, para lograr las bases y las condiciones para obtener valiosos conocimientos.

Daniel Terán

# Tabla de Contenido

# Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la Legislación Argentina desde un enfoque de ciberseguridad y delitos informáticos.


Autor(es):

Cristian Javier Rubio Ganchala

Daniel Alejandro Teran Suarez

# Resumen

El presente documento investigativo analiza y compara la Ley Orgánica de Protección de Datos Personales del Ecuador con la Legislación Argentina, ambas normativas enfocadas en el ámbito de ciberseguridad y delitos informáticos. Esto se lleva a cabo a través de varios ítems detallados secuencialmente, en primer lugar, se describe la importancia que tiene la informática en la actualidad y las vulnerabilidades que trajo el crecimiento tecnológico, con esta información se clasificaron los delitos informáticos más importantes ocurridos en los dos países latinoamericanos: Ecuador y Argentina. Una vez clasificados se examinaron ambas normativas para determinar los artículos que sancionan a cada uno de estos y la penalidad que les corresponde. Seguidamente se elabora una reseña histórica de ambos países con el fin de entender la necesidad que tuvieron en generar una ley que garantice la protección de datos personales de los ciudadanos, y, por último, presenta una serie de recomendaciones que pueden ser consideradas al momento de desarrollar un sistema de gestión de seguridad de la información en las diferentes organizaciones interesadas.

**Palabras clave:**

crecimiento tecnológico, delitos informáticos, datos personales, protección de datos.

# ABSTRACT

This research paper analyzes and compares the Organic Law on Protection of Personal Data of Ecuador with Argentine Legislation, both regulations focused on the field of cybersecurity and computer crime. This is carried out through several sequentially detailed items, first, describes the importance of computing today and the vulnerabilities brought by technological growth, with this information, the most important computer crimes that occurred in the two Latin American countries: Ecuador and Argentina were classified. Once classified, both regulations were examined to determine the articles that sanction each of these and the penalty that corresponds to them. Next, a historical review of both countries is prepared in order to understand the need they had to generate a law to guarantee the protection of citizens personal data, and, finally, presents a series of recommendations that can be considered when developing an information security management system in the different interested organizations.

**Keywords:**

technological growth, cybercrime, personal information, data protection.

# 1. Introducción

En el presente trabajo investigativo se efectúa un análisis comparativo de la normativa jurídica con respecto a la protección de los datos personales de dos países latinoamericanos. Los sistemas jurídicos abarcados son Ecuador y Argentina. El objetivo es analizar y comparar la Ley Orgánica de Protección de Datos Personales de estos dos países desde un enfoque de ciberseguridad y delitos informáticos.

El consumo del internet se ha convertido en una prioridad, el uso de un ordenador es una herramienta de vital importancia para realizar las labores diarias y este crecimiento tecnológico a nivel mundial ha traído consigo ciertas vulnerabilidades informáticas que afectan tanto a las personas como a las empresas. Por ejemplo, en Ecuador a partir del año 2009 se han receptado denuncias relacionadas con la clonación de tarjetas de crédito, robo de contraseñas, ataques a páginas web del gobierno y fraude informático.

El documento identificará los tipos de delitos informáticos más graves que ocurren en Ecuador y Argentina y su penalización en la Ley Orgánica de Protección de Datos Personales de cada país, analizando posibles alternativas de solución para reducir el riesgo de ser víctima de la ciberdelincuencia, tanto a nivel personal como empresarial.

La investigación está estructurada en cuatro capítulos. En el primero de ellos se determina el principal problema, sus causas y posibles soluciones. En el siguiente se revisan los conceptos más importantes que abarcan al tema de estudio, así como también se realiza una pequeña reseña histórica de la protección de datos personales y se aclaran términos que van a ser utilizados para referirse al derecho a la protección de datos. A continuación, en siguiente capítulo se presenta la metodología utilizada para llevar a cabo los análisis comparativos de los dos países latinoamericanos. Finalmente, en el último capítulo se presentan las conclusiones generales del presente estudio.

# 2. Determinación del Problema

El principal tema de este trabajo está centrado en el análisis comparativo de la Ley Orgánica de Protección de Datos Personales (LOPDP) de ambos países y su relación con los delitos informáticos, ya que vulneran y atentan contra los derechos constitucionales de los ciudadanos, y en muchos casos quedan impunes porque es difícil identificar a los perpetradores. Las violaciones de la privacidad de las personas y el mal uso de los datos personales son cada día más fáciles con el desarrollo de las nuevas tecnologías y la globalización.

Los dos países han discutido proyectos de ley destinados a regular la protección de los datos personales y la privacidad de los ciudadanos, pero tomando en cuenta el desarrollo considerable que han tenido las tecnologías de información y comunicación, dichos avances no son suficientes ante la problemática señalada, mediante un panorama que englobe las necesidades que han llevado a estos países a generar una ley que garantice la protección de datos personales e identificando los delitos informáticos tipificados en cada ley. El trabajo también presenta una serie de recomendaciones que podrían ser consideradas al momento de desarrollar un sistema de gestión de seguridad de la información (SGSI) según la legislación de cada país y de esta manera dar una solución a la problemática mencionada.

# 3. Marco teórico referencial

## 3.1 Delitos informáticos

Acosta et al. [1] afirma que los delitos informáticos son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos. Por su parte, Gómez señala que "los delitos informáticos son un conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos" [2]. Ruiz recoge la definición que adopta "El Mercado de la Organización para la Cooperación y el Desarrollo Económico" en la recomendación número R(81) 12 del Consejo de Europa indicando que abuso informático "es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos" [3]. Finalmente, se cita a Parker quien definió el término delito informático como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio" [4].

### 3.1.1 Reseña histórica

Los orígenes de los delitos informáticos pueden rastrearse a partir de los años 60 por el temor infundido por la literatura de la época con relación a la recolección y almacenamiento de datos personales en computadoras. Éste tiene como referencia la obra "1984" de George Orwell, en donde el protagonista conocido como "el omnipresente Gran Hermano" controla y monitorea la vida de las personas a través de las tecnologías.

El término “delito informático” apareció por primera vez después de que se publicaran artículos periodísticos sobre algunos de los delitos más importantes ocurridos en la época, después de un tiempo a este tipo de actos se los denominó como "ciberpunk" [1].

Ya en la década de 1970 se empezaron a documentar varios casos de delitos informáticos los cuales causaron grandes pérdidas al sector privado, los principales fueron: el espionaje informático, la piratería de software, el sabotaje y la extorsión. Desde principios de la década de 1980, los delitos informáticos se dieron a conocer a medida que el número de casos de fraude aumentaba rápidamente y las organizaciones internacionales tomaron cartas en el asunto y abordaron el problema [1].

A mediados de la década de 1990 con la apertura de internet en todo el mundo, organizaciones se centraron en la creación de estándares de cifrado seguro para el desarrollo de operaciones financieras y la compra y venta de productos en línea, ya que empezaron a surgir una serie de infracciones de derechos de autor en las industrias discográficas y cinematográficas relacionadas con la descarga y el intercambio de música y películas en línea, lo que llevo a debates sobre como organizar esfuerzos cooperativos internacionales para evitar filtraciones corporativas [1].

### 3.1.2 Tipos de delitos informáticos

Existen distintos criterios con respecto a la clasificación de los tipos de delitos informáticos existentes; Lara et al. [5] propone la siguiente clasificación:

- El acceso no autorizado

Esto ocurre cuando una persona obtiene acceso no autorizado a cualquier sistema o red violando todas las medidas de seguridad existentes. Suelen estar a cargo de genios informáticos conocidos como piratas informáticos o Hackers.

- El daño a los datos o programas informáticos

Esto incluye el borrado completo, degradación, erradicación de softwares sin que el ejecutante se encuentre autorizado.

- El sabotaje informático

Su finalidad es modificar y borrar por completo datos o programas. Provocan interferencias para evitar que los sistemas informáticos funcionen y, por lo tanto, que funcionen redes enteras.

- La interceptación no autorizada

Se refiere a la recopilación de información sin antes haber tenido una autorización, tomando en cuenta los mecanismos tecnológicos habituales.

- El espionaje informático

Se refiere a la obtención, publicación y transmisión de información confidencial de redes comerciales sin la autorización del dueño de la información con el objeto de causar pérdidas financieras u obtener un beneficio indebido. Luna [6] autora del trabajo "Espionaje informático, robo de identidad e información" asegura que "uno de los delitos de informática más utilizados por los ciberdelincuentes, es el espionaje informático. Explica el autor, que el mismo actúa como acechador, instigador y vigila de manera disimulada, a una persona clave para luego abordarla y obtener información sobre una persona, una empresa o del gobierno. El espionaje industrial, ha cobrado mucho auge mediante la tecnología y, representa una buena plaza donde los cibercriminales pueden obtener mejores ganancias metálicas"

- Riesgos a la sociedad

Estos riesgos surgen de una combinación de circunstancias, a menudo denominadas ataques y amenazas a los sistemas de información. Los tipos de riesgos más comunes son: riesgos de integridad, riesgo de relación, riesgo de acceso, riesgo de servicios públicos, riesgo de infraestructura, riesgo de seguridad general,

centralización de aplicaciones más grandes y complejas, dependencia de personal clave y pérdida de controles tradicionales [1].

Además, Acosta et al. [1] afirma que: “En definitiva, el delito informático es una forma de delinquir extrayendo información personal directamente del ciberespacio, el cual abarca el problema amenazando los entornos privados de la sociedad en general, además de adicionar posibles daños patrimoniales tanto personales como empresariales, producidos por el abuso de datos extraídos. Generalmente tiene carácter transfronterizo, que exige una respuesta adecuada y rápida y, por lo tanto, se necesita actualizar una debida adaptación de las Leyes según la naturaleza del delito y la seguridad adecuada para el resguardo de la información y la defensa del territorio cibernético” [1].

### 3.1.3 Primeros delitos informáticos, autores y sanciones

Uno de los ataques más famosos se dio en el año 1971 y fue denominado como CREEPER, sobre el cual Bob Thomas escribió: “es considerado el primer virus informático que afectó a una computadora el cual mostraba un mensaje en los equipos infectados, si bien no causaba daño alguno, fue la base para el desarrollo de ataques posteriores con pérdidas multimillonarias, como se menciona en el sitio web de la INTERPOL, se estima que en 2007 y 2008 la ciberdelincuencia tuvo un coste a escala mundial de unos 8.000 millones de dólares USD" [3] [8].

En el año 1981, Ian Murphy, conocido como el capitán Zap, hackeó la red de AT&T y cambió el reloj interno para recargar tarifas fuera del horario en horas pico, fue la primera persona condenada por un delito cibernético y recibió como sanción 1.000 horas de servicio comunitario y 2,5 años de libertad condicional [4] [10].

En 1988, Robert Morris creó lo que se conoció como el primer gusano de Internet. “El gusano fue liberado desde una computadora en el Instituto de Tecnología de Massachusetts, lo que sugiere que su creador era un estudiante. Este ataque potencialmente inofensivo se convirtió rápidamente en un ataque masivo de

denegación de servicio cuando una falla en el mecanismo de propagación del gusano hizo que las computadoras se infectaran y volvieran a infectar mucho más rápido de lo esperado". El gusano Morris infectó aproximadamente 6.000 de las 60.000 computadoras conectadas a ARPANET en ese momento. La sanción que recibió fue: 3 años de libertad condicional y una multa de $10.000 USD [5] [10].

Conocido mundialmente como "el hacker más famoso", Kevin Mitnick, fue el primer hacker en ser encarcelado por infiltrarse en un sistema informático. "En 1992, el gobierno acusó a Kevin de robar inteligencia del FBI, estar involucrado en la investigación de Ferdinand Marcos, piratear computadoras militares y convertirse en un símbolo de la comunidad internacional de piratas informáticos" [12]. Fue arrestado en 1995 en Raleigh, Carolina del Norte después de una investigación del FBI de tres años y puesto en libertad en enero de 2000, pasó casi cinco años en una prisión federal a costa de los estados y territorios de EE. UU. Empresas privadas perdieron millones de dólares porque sufrieron robos de software, información y modificación de datos. Entre las víctimas de este delito informático se encuentran empresas como Motorola, Novell, Nokia y Sun Microsystems, el FBI, el Pentágono y la Universidad del Sur de California [12].

El ingeniero de software ruso Vladimir Levin, en el año 1995, hackeó los sistemas informáticos de Citibank en Nueva York desde su domicilio en San Petersburgo y autorizó una serie de transacciones fraudulentas que resultaron en transferencias de aproximadamente $10 millones a cuentas en todo el mundo. Levin fue sentenciado a 3 años de prisión y pagó a Citibank $240.015 USD, porque las compañías de seguros ya habían pagado a las compañías agraviadas [7].

El ataque del gusano WannaCry comenzó el 12 de mayo de 2017, cuando ocurrieron las primeras infecciones en Asia. Por su naturaleza, se propagó como la pólvora, infectando 10.000 equipos por hora y manteniendo ese ritmo hasta que se detuvo cuatro días después. Este ransomware provocó el caos de inmediato, especialmente en hospitales y otros centros de atención médica. "El ataque devastó en NHS y muchos hospitales se vieron obligados a cerrar por completo sus sistema de TI, lo

que afectó la atención al paciente e incluso las operaciones y otras operaciones especiales" [15].

WannaCry se extendió rápidamente a 150 países, sin embargo, no tenía en específico un objetivo. El mayor porcentaje de los incidentes fueron en Rusia, China, Ucrania, Taiwán, India y Brasil, cabe recalcar que muchas personas y organizaciones se vieron afectadas. "WannaCry demandaba a cada usuario el pago de $300 USD en bitcoins (o $600 USD si no se cumplía el plazo inicial), su coste en daños fue muy superior. Unas 330 personas u organizaciones pagaron el rescate, lo que supuso un total de 51,6 bitcoins (unos $130.634 USD al cambio registrado en mayo del 2017)". Esa es la cantidad que se pagó a los piratas informáticos, pero el costo real de WannaCry fue mucho mayor. Debido a la gran cantidad de agencias gubernamentales, universidades e instalaciones médicas involucradas en contención de daños resultante, el costo de la limpieza fue muy alto. Cyence, una empresa de modelado de riesgo cibernético estimó el costo total en $ 4 mil millones [15].

Diario El Telégrafo publicó un artículo acerca de un delito informático ocurrido en la ciudad de Quito, titulado: Caso "Skimmer Uno": Los involucrados fueron detenidos tras el operativo que se ejecutó el 14 de marzo del 2014. El Juzgado Séptimo de Seguridad Penal de Pichincha condenó a seis extranjeros a 12 meses de prisión por su presunta participación en la clonación de tarjetas de crédito y débito. Está organización colocaba en el cajero automático un dispositivo denominado skimmer, con el cual grababan las claves y datos de la banda magnética de las tarjetas [13]. Según las investigaciones, esta banda realizaba en promedio 10 retiros diarios, los mismos que se hacían desde las 23:00. Se estima que los delincuentes retiraban hasta $10.000 USD al día [14].

## 3.2 Hacker

Un hacker es una persona que usa su habilidad con las computadoras para tratar de obtener acceso no autorizado a los archivos informáticos o redes [3].

Sain define el término hacker como: “Aquellos programadores que trabajan en el campo de la informática interactiva para que las computadoras puedan comunicarse entre sí a través de la innovación tecnológica” [15].

De acuerdo con Raymond “es una persona que es experta en un lenguaje de programación, en un programa en particular o en un sistema operativo” [16].

Universalmente el término hacker se usa para quienes intentan irrumpir en los sistemas de computación. Típicamente este tipo de hacker pueden ser expertos programadores o ingenieros con suficiente conocimiento técnico como para hallar los puntos débiles en un sistema de seguridad [9].

### 3.2.1 Clasificación

En el ámbito informático según Loredo [7] los hacker se pueden clasificar en:

- White hat hacker

Se dedican a buscar vulnerabilidades en redes y sistemas sin realizar un uso malicioso de estas y posteriormente reportando los fallos. Las formas en que se monetiza esta actividad son varias: búsqueda de reputación en el sector, sistema de recompensas, trabajar como consultor o responsable de seguridad en una compañía.

- Black hat Hacker

Son individuos con amplios conocimientos informáticos que buscan romper la seguridad de un sistema buscando una ganancia, ya sea obtener bases de datos para su posterior venta en el mercado negro, venta de “xploits” (vulnerabilidades de seguridad), robo de identidad, cuentas bancarias, etc.

## 3.3 ¿Qué es un Sistema de Gestión de Seguridad de la Información?

Según la ISO/IEC 27000 “un SGSI consiste en políticas, procedimientos, directrices, recursos y actividades asociados, los cuales son administrados por una organización, con el objetivo de proteger sus activos de información” [18].

El blog perteneciente al Centro Europeo de Postgrado (CEUPE), publicó un artículo titulado: Política de Seguridad de la Información y SGSI en donde nos indica que: “la seguridad de la información es la protección de la misma contra varios tipos de amenazas para garantizar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de la inversión y las oportunidades comerciales” [20].

También en [23] se enuncia que “la seguridad de la información es el resultado de implementar un conjunto de controles, que incluyen políticas, procesos, procedimientos, estructuras organizaciones y características de hardware y software”.

Dados estos conceptos, a continuación, se mencionan algunos principios referentes a la importancia de los SGSI:

La Superintendencia de Economía Popular y Solidaria de Ecuador [24] menciona las ventajas que trae la implementación de un Sistema de Gestión de Seguridad de la Información en cualquier organización:

- Incluye un compromiso por parte de la gerencia y partes interesadas
- Realiza evaluaciones de riesgos para determinar las medidas de control apropiadas para lograr un nivel de riesgo aceptable.
- Mantiene a la seguridad como un parámetro esencial de las redes y sistemas de información.
- Previene de forma proactiva cualquier tipo de incidente.
- Asigna responsabilidades a quien corresponda, así toda la organización trabaja en conjunto.

- Asegura que tenga un enfoque integral, lo que significa que existirá una reevaluación continua y actualizada.

## 3.4 ¿Qué es una ley orgánica?

Se entiende por ley orgánica un instrumento de ordenamiento jurídico, cuyo objeto es determinar las bases de la organización y funcionamiento de las instituciones derivadas de los tres poderes del Estado. Analizando constitucionalmente, la ley orgánica tiene como principal objetivo la regulación de ciertos aspectos de la vida social, la mayoría de las veces son vistas como un conector entre el derecho consuetudinario y la constitución para promover el buen funcionamiento de las instituciones estatales [12].

Bulnes establece que para Chile una ley orgánica es "una norma que, estando prevista como tal en la Constitución Política para la aprobación de ciertas materias, necesita, para ser aprobada, modificada y derogada, del quórum de tres quintos de los Diputados y Senadores en ejercicio, o de la unanimidad de la Honorable Junta de Gobierno, en el período de transición; que no procede, a su respecto, la delegación de facultades legislativas en el Presidente de la República; y que es obligatorio el control previo de su constitucionalidad por el Tribunal Constitucional, antes de su promulgación" [21].

### 3.4.1 ¿Cuándo es necesario proponer una nueva ley en el país?

Según Pérez et al. [22] en los siguientes casos es necesario: Como ente regulador tanto de los derechos como de las garantías constitucionales; crear, editar o eliminar atributos; cambiar la división política y administrativa del país; clasificar las infracciones y determinar las sanciones pertinentes; asignar responsabilidades, rendición de cuentas y autoridad a los GADs y por último cuando los organismos públicos de control y regulación lo consideren necesario [25].

## 3.5 Reseña histórica de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP)

La LOPDP se presentó como una iniciativa de proyecto de ley el 19 de septiembre de 2019 por parte del entonces Presidente de la República del Ecuador Lic. Lenin Moreno, esto debido a las noticias de la mayor filtración de datos que había ocurrido en el Ecuador y que posiblemente involucró a ex funcionarios de Gobierno (Instituciones Públicas) de lo cual, hasta la fecha de esta publicación, se tiene conocimiento únicamente de una denuncia en fiscalía; una vez que el ex Presidente entregó el proyecto de ley este fue tratado al interior de la Comisión de Relaciones Internacionales y Movilidad Humana de la Asamblea Nacional [13].

Con 118 votos a favor, el pleno de la Asamblea Nacional aprobó el 10 de mayo de 2021, la Ley de Protección de Datos Personales. Este cuerpo legal pasó por un amplio proceso de construcción participativa, el cual inició en octubre de 2017.

La construcción de la Ley se realizó en conjunto con varios sectores públicos y privados expertos en la materia. Como parte de esto se desarrollaron varias mesas de trabajo con instituciones públicas del sector de las telecomunicaciones, tales como Agencia de Regulación y Control de las Telecomunicaciones (Arcotel), Agencia de Regulación y Control Postal (ARCPostal), Correos del Ecuador EP, Corporación Nacional de Telecomunicaciones (CNT), Registro Civil y Ministerio de Telecomunicaciones y de la Sociedad de la Información (Mintel). Expertos nacionales e internacionales participaron en las mesas de trabajo con el fin de analizar esta iniciativa legal [27].

Las organizaciones públicas y privadas tuvieron un plazo máximo de dos años para poner en marcha procedimientos internos con el fin de cumplir con la LOPDP, es decir hasta el 22 de mayo de 2021. La aprobación de la LOPDP brindará a las entidades privadas y empresas que tratan datos (bases de datos) la oportunidad de

establecer normas y sus medidas técnicas y organizativas que deben implementar para que los datos a su disposición sean debidamente protegidos y utilizados [27].

La Ley de Protección de Datos Personales fue aprobada por la Asamblea Nacional el 10 de mayo de 2021 y publicada en la Gaceta Legislativa el 26 de mayo del mismo año [14] [27].

## 3.6 Reseña histórica de la Ley de Protección de Datos de Argentina

La República Argentina reformó la Constitución Nacional (CN) en 1994. En esta constitución se aprobó un nuevo capítulo titulado "Nuevos derechos y garantías", Algunos de los cuales están consagrados en la legislación y la jurisprudencia. Este nuevo capítulo de la constitución complementa al capítulo primero, el cual abarca las clásicas y siempre vigentes “declaraciones de derechos y garantías de las constituciones históricas” [29].

Con las reformas constitucionales antes mencionadas, se incluyó entre estas normas el artículo 43, cuya tercera parte tiene en cuenta el llamado habeas corpus data, de la siguiente manera: “Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística”. Luego de este evento, la Asamblea Nacional adoptó el alcance del mencionado artículo 43 de la Constitución por una ley nacional y en 2000 aprobó la Ley núm. 25,326 [29].

Una de sus características fundamentales es que es una ley de orden público, entonces no puede ser anulada por la voluntad del pueblo. Es importante mencionar que, el Ejecutivo Nacional cumplió con sus deberes con el decreto reglamentario de la Ley N° 25.326: protección de datos personales, establecimiento

de control legal, único control legal en América Latina y el tercer mundo (hemisferio sur) [29].

De esta manera, se comprueba la potestad de este proceso de cambio desde el poder constitucional a través del poder legislativo, ejecutivo y judicial, lo que significa que en Argentina se cristaliza, acelera, dinamiza y distribuye la concreción de la protección de datos personales. La constitución y las regulaciones de Argentina brindan un marco efectivo para proteger la reputación y la privacidad de los datos [29].

## 3.7 Datos Personales

La Unión Europea lo define como: "Cualquier información sobre una persona física identificada o identificable, es decir, cualquier persona cuya identidad pueda determinarse directa o indirectamente, en particular por medio de un identificador como nombre, número de identificación, datos de ubicación, identificador en línea o elementos físicos, fisiológicos, uno o más genéticos, mentales, económicos, de identidad cultural o social" [16].

### 3.7.1 ¿Cuáles fueron los primeros países que aprobaron una ley de protección de datos?

Las primeras leyes de protección de datos se adoptaron en 1970. Según Suñé, las propiedades originales correspondían al estado registrado en la ex República Federal de Alemania. Luego, en 1973, Suecia aprobó la Ley de Protección de Datos. Luego, Estados Unidos aprobó su propia ley en 1974. Esto fue seguido en 1976 por Nueva Zelanda y Canadá, y en el mismo año por la constitucionalidad de la protección de datos personales de Portugal. En 1977, se adoptó la Ley Federal de Protección de Datos en la República Federal de Alemania. El año siguiente vio la mayor ola de legislación en la Europa libre, con leyes aprobadas en Francia, Noruega, Dinamarca, Austria y España adoptaron una nueva constitución que prevé la protección de datos personal [31].

### 3.7.2 ¿Cuáles fueron las necesidades que dichos países experimentaron para proponer una LPDP?

Surgió como un mecanismo legal para proteger el derecho a la privacidad de las personas en la era de la tecnología de la información. Sus objetivos principales son: definir los datos personales; determinar quién es el responsable del procesamiento de datos; regular cuestiones básicas del tratamiento de datos, tales como almacenamiento, acceso, seguridad, confidencialidad; y establecer un nivel adecuado de protección para la transferencia de datos personales a otros países [18].

# 4. Materiales y metodología

## 4.1 Enfoque de la investigación

### 4.1.1 Tipo de investigación

El trabajo de investigación a realizar utilizará principalmente la revisión y análisis de bibliografía, abarcando un cierto nivel de conocimiento descriptivo: Según Baena "La investigación documental es una técnica que consiste en la selección y recopilación de información por medio de la lectura y crítica de documentos y materiales bibliográficos, de bibliotecas, hemerotecas, centros de documentación e información" [19]. Los siguientes puntos de investigación utilizarán fuentes primarias y secundarias de información.

Primaria: "Ley Orgánica de Protección de Datos Personales del Ecuador" y la "Ley de Protección de Datos Personales N° 25.326".

Secundaria: Tesis, libros, artículos de revistas y periódicos, publicaciones oficiales de sitios web, resúmenes de trabajos científicos y reportajes; en donde todos hagan énfasis en el ámbito relacionado a la ciberseguridad y delitos informáticos.

El nivel de conocimiento descriptivo en el proyecto de investigación se verá reflejado en un análisis comparativo de la legislación que rige sobre ambos países latinoamericanos desde el enfoque de la ciberseguridad y la evaluación de la situación real de Ecuador y Argentina con respecto a los Sistemas de Gestión de Seguridad de la información, lo que permitirá obtener lineamientos para deducir el funcionamiento de estos sistemas en ambos países latinoamericanos y la manera en la que se deben ir acoplando a los sistemas que actualmente utilizan las organizaciones tanto ecuatorianas como argentinas.

La información recopilada se puede utilizar para el análisis cualitativo para identificar y comprender la gravedad de los problemas hipotéticos o parcialmente conocidos.

### 4.1.2 Diseño de la investigación

La investigación será de carácter no experimental, ya que la información registrada será utilizada en diversas iniciativas legales en dos países latinoamericanos (Ecuador y Argentina) para proteger datos personales en los últimos años. Para ello, se analizarán los documentos legales elaborados por las distintas unidades estructurales del sector público (legislación específica de cada país), decretos, propuestas legislativas, comentarios y aportes.

## 4.2 Metodología

### 4.2.1 Recolección de datos

En la fase de investigación, se recopilará información de fuentes primarias y secundarias. En primer lugar, se analizarán diversas iniciativas legales en materia de protección de datos personales en dos países latinoamericanos (Ecuador y Argentina) en los últimos años. Para ello se analizarán los documentos legales (legislación propia de cada país), decretos, proyectos de ley, comentarios y aportes elaborados por diversas unidades del sector público, pero en cuanto a fuentes secundarias serán documentos, libros, revistas científicas con artículos sobre Ciberseguridad y delitos en Internet.

### 4.2.2 Recursos

Equipos y materiales: En el marco del proyecto se realizará una investigación documental y descriptiva, utilizando principalmente una computadora con sus respectivos softwares.

Recursos bibliográficos: Se utilizarán documentos con validez técnica y científica como: tesis, libros, sitios web, normativas legales sobre la protección de datos personales, leyes e información referente al caso de estudio.

### 4.2.3 Materiales y métodos

La técnica que se utilizará en el trabajo investigativo será documental la cual consiste en una serie de actividades que se lleva a cabo una vez seleccionado el tema con el fin de localizar, seleccionar, organizar y analizar los datos que permiten comprender el estado del problema, es decir, la investigación realizada y los resultados obtenidos [20].

El método será aplicado a cada objetivo establecido para realizar el trabajo.

Para el cumplimiento del primer objetivo se utilizará la información obtenida de diferentes fuentes a lo largo de los años y a nivel mundial de proyectos de ley que han procurado regular la protección de los datos personales y la privacidad. Se ha presentado una reseña histórica donde se plasman los diferentes delitos informáticos ocurridos en un orden cronológico, con su respectivo país y autor; analizando la reseña se conocerá las necesidades a nivel mundial de la importancia de proteger a las personas de posibles amenazas a estos derechos en el entorno digital. Esta sección analiza los debates y el proceso legislativo en los últimos años sobre diversas iniciativas legales para la protección de datos.

Con respecto al segundo objetivo, a partir de la reseña histórica obtenida que engloba a todos los delitos informáticos a nivel mundial se ha trabajado sobre una muestra representativa con características similares centrándose en los países de Ecuador y Argentina, lo cual ha permitido elaborar una tabla que refleje los artículos, el enunciado y la sanción en cada caso.

Para desarrollar el tercer objetivo se ha partido del análisis realizado en los puntos anteriores acerca de la importancia de la protección de datos personales y las leyes existentes que lo rigen, esto permitirá obtener un diagnóstico inicial de cómo operan y funcionan los Sistemas de Gestión de Seguridad de la Información en los diferentes países y de esta manera proporcionar ajustes o recomendaciones que se consideren necesarias, las cuales podrán ser tomadas como referencia y guía ya que agrupará procedimientos puntuales con un objetivo común.

## 4.3 Delitos Tipificados en la Ley de Protección de Datos Personales en Argentina y Ecuador

La revista Líderes, señala que “el delito informático más cometido en el Ecuador fue el fraude bancario, los que han sido mayormente reportados han sido la clonación de tarjetas de crédito o débito y así mismo el robo de contraseñas” [31].

Dentro de los delitos tipificados existen casos de transacciones virtuales no autorizadas, que ocurren cuando las víctimas intentan realizar transacciones o actualizar datos en sitios web falsos creados por ciberdelincuentes que quieren ganar dinero obteniendo las contraseñas de las cuentas bancarias de las víctimas, retirando dinero hasta que la cuenta bancaria esté vacía [36].

Otro ciberdelito es común suele ser llevado a cabo por los famosos piratas informáticos, quienes provocan la inactividad temporal de ciertos servicios web públicos, como los experimentados por entidades como: Secom, Senami, Magap, Telecom, Relaciones Industriales y el sitio web del presidente de Ecuador [36].

Existe una larga lista de los delitos informáticos ocurridos en Ecuador, entre los más importantes tenemos: la interceptación ilícita, accesos no autorizados, ataques a la integridad de datos y sistemas, abuso de dispositivos, falsificación y fraude informático, delitos contra la propiedad intelectual y la pornografía infantil [22] y [36].

Diario El Comercio asegura que: “Los ataques de las cibermafias son recurrentes en el país. Un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado 3.183 delitos informáticos. En todo el 2020 fueron 682 casos; en el 2021 subieron a 1.851 y en poco más de seis meses de 2022 la Policía ya ha iniciado 650 investigaciones a escala

nacional. Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay son las provincias con más casos" [23].

Es importante mencionar que en Ecuador existe una ley que regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas [37]. A continuación, se detallan dos artículos que se encuentran en la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

**Art. 5. Confidencialidad y reserva:** "Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia" [38].

**Art. 9. Protección de datos:** "Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros" [38].

En caso de violar los derechos anteriormente expuestos existe una sanción para ambos casos: "La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción: amonestación escrita, multa de $500 a $3000 dólares, suspensión del cargo [33].

Según Philco et al. [34]: "Se sancionan los delitos informáticos que implican intentos de comprometer la seguridad de la información confidencial, divulgación ilegal de datos, pérdida financiera, acceso no autorizado". La Tabla 1 resume las reglas, las acciones punibles y las sanciones para los infractores.

**Tabla 1. Delitos informáticos tipificados en la legislación ecuatoriana**

| Artículo | Código Orgánico Integral Penal del Ecuador | Sanción |
|---|---|---|
| **Art 103.** Comercialización de pornografía | "La persona que publicite compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio". | De 10 a 13 años de prisión. |
| **Art 174.** Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos | "La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad". | De 7 a 10 años de prisión. |
| **Art 178.** Violación a la intimidad | "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos". | De 1 a 3 años de prisión. |
| **Art 186.** Estafa | "Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares". | De 5 a 7 años de prisión. |
| **Art 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". | De 1 a 3 años de prisión. |
| **Art 229.** Revelación ilegal de base de datos | "La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones". | De 1 a 3 años de prisión. |
| **Art. 230** Interceptación ilegal de datos | "La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen". | De 3 a 5 años de prisión. |
| | "La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, 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". | |
| | "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". | |
| | "La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior". | |
| **Art 231.** Transferencia electrónica de activo patrimonial | "La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero". | De 3 a 5 años de prisión. |
| **Art 232.** Ataque a la integridad de sistemas informáticos | "La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones". | De 3 a 5 años de prisión. |
| **Art.233.** Delitos contra la información pública reservada legalmente | "La persona que destruya o inutilice información clasificada de conformidad con la Ley". | De 5 a 7 años de prisión. |
| | "La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información". | De 3 a 5 años de prisión. |
| | "Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información". | De 7 a 5 años de prisión y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad. |
| **Art. 234.** Acceso no consentido a un sistema informático, telemático o de telecomunicaciones | "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, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer | De 3 a 5 años de prisión. |

| | | |
|---|---|---|
| | servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos" [39]. | |

Dentro de la ley argentina de Protección de Datos Personales, existen artículos que respaldan el derecho de los ciudadanos:

**Art.9. Seguridad de los datos:**

"El responsable o usuario de los ficheros de datos deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal, evitar su manipulación, pérdida, consulta o tratamiento no autorizado y permitir la detección de desviaciones intencionadas o accidentales. , con independencia de que el riesgo sea causado por la actividad humana o por los medios tecnológicos utilizados. Prohibición de registrar datos personales en archivos, registros o bancos que no reúnan las condiciones técnicas de integridad y seguridad" [41].

**Art 10. Deber de confidencialidad:**

"Cuando se presten servicios de tratamiento de datos personales por cuenta de terceros, éstos no podrán ser utilizados ni utilizados para fines distintos a los especificados en el contrato de servicios, cedidos a otra persona ni siquiera almacenados. En tales casos, la autoridad de control podrá aplicar apercibimientos, suspensión, multas de mil pesos ($1.000) a cien mil pesos ($100.000), cierre o cancelación de documentos, registros o bases de datos. La siguiente tabla describe el panorama global de la regulación del delito cibernético en Argentina" [41].

La Tabla 2 presenta un resumen de los principales delitos informáticos tipificados en le ley argentina:

**Tabla 2. Delitos informáticos tipificados en la legislación argentina**

| Artículo | Código Penal Argentino LEY 11.179 | Sanción |
|---|---|---|
| Capítulo II. Delitos contra la integridad sexual | | |
| **Art 128.** | produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. | Será reprimido con prisión de seis (6) meses a cuatro (4) años |
| **Art. 131.** | Por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, tomare contacto con una persona menor de edad, con el propósito de cometer cualquier delito contra su integridad sexual | Prisión de cuatro meses a seis años |
| Capítulo III. Violación de Secretos y de la privacidad | | |
| **Art 153.** | abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido | Será reprimido con prisión de quince (15) días a seis (6) meses |
| **Art. 153 BIS** | El que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. | Será reprimido con prisión de quince (15) días a seis (6) meses |
| | Cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. | La pena será de un (1) mes a un (1) año de prisión |
| **Art. 155** | El que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. | Será reprimido con multa de mil quinientos ($ 1.500) pesos cien mil ($ 100.000) pesos |

| | | |
|---|---|---|
| **Art. 157** | El funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos. | Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años |

Mediante la elaboración de las tablas se logró tener una visión general de los principales delitos informáticos tipificados tanto en la normativa ecuatoriana como argentina. Se ha analizado los artículos relacionados con la ciberseguridad que sanciona los delitos informáticos, llegando resumiendo su definición y correspondiente sanción.

## 4.4 Recomendaciones a considerar para el desarrollo de un SGSI acorde a la normativa analizada

En este apartado del trabajo investigativo se redactará una serie de lineamientos que es importante tomar en cuenta al momento de desarrollar un SGSI, para esto se analizó la normativa de cada país con el objetivo de garantizar el tratamiento de los problemas de seguridad de la información.

A través de esta serie de recomendaciones se busca dar un aporte a cualquier organización que quiera implementar un SGSI garantizando que estas tomen medidas para mantener seguros los datos y la información de los ciudadanos.

Todas estas recomendaciones abordaran los requerimientos de cumplimiento de las leyes de protección de datos personales en Ecuador y Argentina.

Tomando en cuenta las recomendaciones brindadas, al momento de desarrollar un SGSI, permitirán a las organizaciones sean más resistentes a los ciberataques, la mejora continua, el énfasis en el monitoreo y la auditoría, lo que permitirá que los dispositivos de control estén siempre actualizados y funcionen de manera óptima.

Mediante estas recomendaciones se busca agrupar un conjunto de procesos que permitan gestionar eficientemente la accesibilidad de la información, de tal manera que sea posible reducir los riesgos de seguridad de la información al garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

A continuación, se presentan las recomendaciones:

Analizar la situación actual de la organización desde un enfoque de ciberseguridad con el fin de tener un panorama global de ciertos puntos que deben ser reforzados o mejorados. Dentro de este punto es importante entender y conocer los parámetros requeridos dentro de la normativa con el fin de que se garantice la seguridad de los datos personales de los ciudadanos.

Identificar cuáles van a ser los activos a proteger, como lo harán y quienes serán los encargados de llevarlo a cabo, es importante establecer responsables de seguridad, políticas de seguridad y los recursos necesarios para la operación, mantenimiento y mejora.

Considerar las necesidades y expectativas de las partes interesadas, esto se lo podría conocer aplicando una encuesta a la ciudadanía en general para conocer que necesitan para sentirse seguros, podría considerarse como un elemento básico el conocer la opinión de la ciudadanía, pero esto nos llevará a que está iniciativa sea un éxito y se mantenga el SGSI dentro de la empresa.

Determinar el alcance que va a tener el sistema de SGSI, teniendo en cuenta los problemas internos y externos de la organización, basándose en las actividades o procesos más importantes dentro de la misma, es decir seleccionar los elementos críticos que se deben proteger y el alcance debe encontrarse disponible como información documentada.

Identificar riesgos y vulnerabilidades de naturaleza crítica de la seguridad de la información dentro de la organización, creando políticas, declaración de aplicabilidad y un plan de tratamiento de riesgos y en base a esto evaluar y definir controles que podrían ser revisiones o evaluaciones continuas.

Analizar la posibilidad de evitar riesgos tomando medidas proactivas y que controles se pueden administrar para proteger mejor los datos de la empresa y al mismo tiempo describir medidas de seguridad que debe tomar la organización para seguir operando de una manera correcta.

Cumplir con las regulaciones de protección de datos de acuerdo a su normativa, es importante realizar un seguimiento de todos los requisitos de estas regulaciones, documentar pasos de acción y realizar revisiones periódicas.

Los controles de acceso a los datos deben ser más estrictos para preservar la confidencialidad de los usuarios y estrictamente contratar un software integral de seguridad con el fin de proteger la información ante los posibles ataques externos a través del internet.

Realizar revisiones del cumplimiento técnico, esto se refiere a revisar periódicamente los sistemas de información para determinar que se estén cumpliendo con las políticas y normas de seguridad de la información.

Una vez implementado el SGSI es importante verificar el funcionamiento de este, esto se lo debe hacer mediante una evaluación, auditoría y certificación con el fin de garantizar que se están siguiendo los protocolos necesarios y que cumple con los lineamientos estipulados.

Realizar revisiones del cumplimiento técnico, esto se refiere a revisar periódicamente los sistemas de información para determinar que se estén cumpliendo con las políticas y normas de seguridad de la información.

Se debe tener un reglamento interno adecuado con lo que respecta al tema de desechos (equipos en desuso donde se almacena información de los clientes); se procede a darles de baja cuando se migre la información a nuevos dispositivos que estén en vigencia; después de hacer esto se procederá con eliminación física del equipo obsoleto, existiendo de por medio veedores para que se asegure así la no fuga de información.

Se recomienda que una vez digitalizada la información que se obtiene a través de documentos físicos, se proceda a la eliminación de estos por medio de triturado o incineración; de esta manera se minimizará el impacto de fuga de información.

Se recomienda colocar cláusulas de confidencialidad de la información de la empresa en los contratos del nuevo personal, en donde quede claramente especificado el alcance legal del mismo (antes, durante y después del contrato) a fin se considere como prioridad la protección de datos de los clientes.

Se recomienda que la gestión de contraseñas sea responsabilidad del encargado del departamento informático; cada contraseña tendrá el respectivo alcance a la información de acuerdo con el perfil profesional de cada empleado, de esta manera nos aseguramos de que la información se maneje por niveles de conocimiento.

# 5. Resultados y discusión

Al redactar la reseña histórica sobre las necesidades que han llevado a Argentina y Ecuador a generar una ley que garantice la protección de los datos personales de los ciudadanos se obtuvo como resultado que ambos países latinoamericanos les surge esta necesidad debido al creciente desarrollo tecnológico en ámbitos de información y comunicación. Todo esto sucede debido a que con el pasar de los años las legislaciones vigentes en ambos países no eran suficientes para resguardar a los individuos de posibles amenazas en el ámbito de delitos informáticos, ya que el mundo se empezó a desarrollar en un entorno digital y así mismo se conoce que diferentes instituciones ya sean privadas o públicas tenían la libertad de acceso a los datos e información personal de los usuarios. Por tal motivo en ambos países se propusieron reformas legislativas específicas con el fin de resguardar la seguridad de los datos personales de los individuos.

Para lograr identificar los delitos informáticos tipificados en la legislación de ambos países el procedimiento realizado se basó en la recolección de información bibliográfica de fuentes primarias y secundarias, obteniendo como resultado que los principales delitos informáticos que han sucedido y sigue pasando en ambos países y en mayor porcentaje son los siguientes: clonación de tarjetas, transacciones virtuales no autorizadas, ciberdelitos contra la intimidad, falsificación y fraude informático, delitos contra la propiedad intelectual, pornografía, virus informáticos y revelación ilegal de base datos.

En el apartado anterior se redactó una serie de recomendaciones que se podrían considerar al momento de desarrollar un sistema de gestión de seguridad de la información en cualquier empresa, analizando estos lineamientos y poniéndolos en práctica se obtendría como resultado: una reducción de riesgos ya que se identificarían los riesgos y amenazas de manera eficaz mediante controles,

protocolos, políticas y monitorización de proceso logrando así reducir el número de amenazas de manera notable; integración de la seguridad en el negocio pasando a ser está uno de los componentes más importantes en todo proceso y actividad de la empresa; uno de los aspectos más importantes que se logra es el cumplimiento de la normativa vigente en seguridad basándose en las leyes de cada país para el tratamiento y protección de datos garantizando que se cumplan en todos los niveles y áreas de la empresa, de esta forma se conseguirá un incremento en la competitividad de la misma, logrando que los clientes se sientan más confiados y seguros de compartir sus datos personales.

Actualmente sigue siendo proceso de discusión y debate la necesidad de actualizar y mejorar las normativas vigentes existiendo de esta manera una protección del derecho a la intimidad mediante la regulación del tratamiento de datos personales, se debe tener en cuenta en que a medida que el derecho a la libertad de expresión fue incluido esté afecta de sobremanera a la circulación de información en internet. Los datos personales son el nuevo petróleo de Internet y la nueva moneda de la economía digital. El desarrollo acelerado de la tecnología también ha creado ciertas lagunas. Es especialmente importante que la normativa de protección de datos se adapte a estos cambios. Es necesario proteger los datos personales, equilibrar el desarrollo económico y la innovación.

Por otro lado la regulación sobre la protección de datos personales que actualmente se desarrolla en América Latina, se debe a varias razones: una de las más importantes es la que impone la globalización económica por lo que es imprescindible encontrar un punto medio entre los intereses económicos, los cuáles cada vez exigen mayores transferencias internacionales de datos, junto con un tratamiento adecuado para ellos, ya que su protección es un derecho fundamental de los usuarios y de esta manera ninguna de las dos partes se vean afectadas.

# 6. Conclusiones

En este trabajo investigativo se realizó un análisis comparativo de la Ley Orgánica de Protección de Datos Personales en dos países latinoamericanos: Argentina y Ecuador. Se hizo énfasis en el nivel de ciberseguridad y delitos informáticos. Se encontró algunas similitudes y diferencias entre ambas leyes. Entre las similitudes se evidenció que en ambos países las dependencias del Poder Ejecutivo encargadas de estos temas dieron cabida a la actualización del marco normativo basadas en el Reglamento General de Protección de Datos de la Unión Europea.

Los delitos informáticos llegan a afectar a todos los usuarios, tanto a las empresas como a las personas que usan tecnología e internet, por este motivo es necesario adoptar medidas de seguridad para minimizar posibles amenazas informáticas una de las posibles soluciones es implementar un sistema de gestión de seguridad de la información para que tanto empresas como usuarios se sientan seguros.

A través del análisis de las leyes de protección de datos personales en ambos países latinoamericanos, se determina que la evolución normativa en materia de protección de datos se ve influenciada por dos factores, en primer lugar, la creciente integración comunitaria y el crecimiento exponencial de los servicios informáticos y telemáticos.

La protección de datos personales en el ordenamiento jurídico argentino es garantizada por vía constitucional y legal. La reforma a la constitución del año 1994 que consagra la denominada acción del hábeas data fue fundamental para el desarrollo de una legislación consistente de protección de datos personales, la cual fue plasmada en la Ley 25.326. En conclusión, puede decirse que la legislación argentina cumple los lineamientos internacionales de protección de datos personales, ya que no solo plantea normas sino también la creación de un organismo de control y destaca ampliamente el régimen de responsabilidad establecido el cuál aplica sanciones administrativas hasta sanciones penales.

Con respecto al ordenamiento jurídico ecuatoriano, sabemos que la Constitución reconoce un derecho a la protección de datos personales y existe una normativa general de protección de datos personales que establece sanciones administrativas.

A criterio de los autores de este trabajo, la Ley Orgánica de Protección de Datos Personales de Ecuador y Argentina, el estándar argentino es más estricto que el implementado en Ecuador, ya que su sistema genera una imagen de seguridad fuerte en la protección de la privacidad, tratamiento y circulación de datos y el modelo ecuatoriano se basa únicamente en la autorregulación del usuario lo que podría traer consigo limitaciones.

Al momento de implementar un SGSI, tomando en cuenta las recomendaciones enunciadas anteriormente por los autores, la organización que las adopté tendrá varias ventajas con respecto a la competencia, principalmente se tendrá como indicador clave analizar de manera global todos los puntos que deben ser reforzados y mejorados en base a la normativa lo que garantizará y regulará la seguridad de los datos personales de los usuarios; otro aspecto importante es que se consideran las necesidades y expectativas por parte de las partes interesadas lo cual es un plus que adquirirá la organización, en caso de no adoptar dichas recomendaciones es que el SGSI no tendrá un alcance acorde a lo que el usuario necesita para que se sienta seguro, ya que no se conocerá su opinión y mucho menos los problemas internos y externos de la organización impidiendo conocer los elementos críticos que deben ser protegidos.

# Referencias


[1] M. G. Acosta, M. M. Benavides y N. P. García, «Delitos Informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios,» Revista Venezolana de Gerencia, Venezuela, 2020.

[2] M. Gómez, «Los Delitos Informáticos en el Derecho Español,» Aranzandi, Mérida, 1992.

[3] E. Ruiz, «Tratamiento de la delincuencia informática como una de las expresiones de criminalidad económica,» Poder Judicial número especial IX, 1989.

[4] D. B. Parker, «Cryme by computer,» New York, 1976.

[5] J. Lara, M. Martínez y P. Viollier, «Hacia una regulación de los delitos informáticos basada en la evidencia,» *Revista Chilena de Derecho y Tecnología,* vol. 3, nº 1, pp. 101-137, 2014.

[6] V. Luna, «Espionaje informático, robo de identidad e información,» Quanti Solutions , México, 2018.

[7] J. A. Loredo y A. Ramírez, «Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo,» Universidad Autónoma de Nuevo León, México, 2013.

[8] «Delitos Cibernéticos,» 06 abril 2017. [En línea]. Available: https://delitosciberneticos19.blogspot.com/2017/. [Último acceso: 2022].

[9] P. Rinaldi, «¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético,» 27 Abril 2017. [En línea]. Available: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/#comments.

[10] Centro Estadístico de Observación y Monitoreo de Cibedelitos, «Historia del Cibercrimen,» [En línea]. Available: https://ogdi.org/historia-del-cibercrimen. [Último acceso: 2022].

[11] Redacción KeepCoding, «KeepCoding Tech School,» 11 agosto 2022. [En línea]. Available: https://www.keepcoding.io.

[12] Madrin News, «Información del Mundo,» 11 Mayo 2011. [En línea]. Available: https://www.mdrinc.wordpress.com.

[13] Observatorio Guatemalteco de delitos informáticos, «Centro Estadístico de Observación y Monitoreo de Ciberdelitos,» 2020. [En línea]. Available: https://www.ogdi.org.

[14] N. Latto, «Avast Academy,» 2020.

[15] N. Latto, «¿Qué es WannaCry?,» RANSOMWARE, España, 2020.

[16] «Fiscalía General del Estado,» 18 Agosto 2014. [En línea]. Available: https://www.fiscalia.gob.ec/seis-sentenciados-a-12-meses-de-prision-en-el-caso-skimmer-uno/. [Último acceso: 2022].

[17] El Telégrafo, «Banda instalaba microcámaras en cajeros para clonar tarjetas,» 14 marzo 2014. [En línea]. Available: https://www.eltelegrafo.com.ec.

[18] G. Sain, «¿Qué es un hacker?,» Revista Pensamiento Penal, 2015.

[19] E. S. Raymond, «The New Hacker's Dictionary,» Third Edition, Estados Unidos, 1995.

[20] N. D. Duque y A. Tamayo, «Hackers, Crackers y otros,» Revista Departamento de Ciencias, Colombia, 2000.

[21] ISO/IEC 27000:2018, «Sistema de Gestión de Seguridad de la Información,» ANSI, 2018.

[22] BLOG CEUPE, «Política de Seguridad de la Información y SGSI,» *CEUPE MAGAZINE.*

[23] «Metodología para la Gestión de la Seguridad Informática,» Oficina de seguridad para las redes informáticas, 2013.

[24] Superintendencia de economía popular y solidaria, «Sistema de Gestión de Seguridad de la Información (SGSI),» SEPS, Quito, 2021.

[25] F. Berlín, «Ley Orgánica,» de *Diccionario Universal de Términos Parlamentarios*, México, Cámara de Diputados del H. Congreso de la Unión, 1997, pp. 420 - 421.

[26] L. Bulnes, «La ley orgánica constitucional,» Universidad de Chile, Chile, 1964.

[27] Pérez, Bustamante y Ponce, «¿Cómo se crean las leyes en el Ecuador?,» Consejo Editorial, Ecuador, 2015.

[28] D. Calvopiña, R. Enriquez, G. Guaman y G. Pacheco, «Cómo se crean las leyes en el Ecuador,» Universidad Central del Ecuador, Quito.

[29] J. Guerrón, «Ecuador y su primera Ley Orgánica de Protección de Datos Personales,» AEC GOVERTIS, Quito, 2021.

[30] Dirección de comunicación social, «Ecuador cuenta con ley de protección de datos personales,» Gobierno del Ecuador, Quito, 2021.

[31] Dirección de Comunicación Social, «Dirección Nacional de Registros Públicos,» 9 Noviembre 2021. [En línea]. Available: https://www.registrospublicos.gob.ec. [Último acceso: 7 Octubre 2022].

[32] J. A. Travieso, «Derecho a la protección de los datos personales,» Argentina, 2017.

[33] L. Enríquez, «Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales,» Revista de derecho, Ecuador, 2021.

[34] L. S. Silva, «EL PORTAL DATO SEGURO Y EL DERECHO DE CONFIDENCIALIDAD DE LA INFORMACIÓN PERSONAL,» Universidad Técnica de Ambato, Ambato, 2016.

[35] L. G. Riascos, «Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009,» Facultad de Derecho y Ciencias Sociales, España, 2012.

[36] G. Baena, «Que es la invesigación documental: Definición y objetivos,» Revista de la Facultad de Ciencias Jurídicas y Políticas, 1985.

[37] I. P. Alvárez Cardona, «Técnicas e Instrumentos para la Recolección de Información,» *Revista de la Facultad de Ciencias Jurídicas y Políticas de una Universidad Fermín Toro,* p. 28, 2012.

[38] EL COMERCIO, «3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020,» *EL COMERCIO,* 25 Julio 2022.

[39] J. V. Enriquez y Y. C. Alavardo, «LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN ELCÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO,» SATHIRI, Carchi, 2015.

[40] M. Flores, «Análisis sobre el comercio electrónico,» Universidad Regional Autónoma de Los Andes, Puyo, 2017.

[41] Congreso Nacional, «Ley de comercio electrónico, firmas electrónicas y mensajes de datos,» LEXIS, Quito, 2002.

[42] A. O. Philco y L. Rosero, «Los Riesgos en Transacciones Electrónicas en Línea y la Criptografía Como Modelo de Seguridad Informática,» Gaceta Sansana, Ecuador, 2014.

[43] Asamblea Nacional, «Código Orgánico Integral Penal, COIP,» Lexis Finder, Quito, 2021.

[44] Congreso Argentino, «PROTECCION DE LOS DATOS PERSONALES: Ley 25.326,» Buenos Aires, 2000.

[45] Congreso Nacional Argentino, «Código Penal de la Nación Argentina. Ley 11.179,» 1984. [En línea]. Available: https://www.oas.org/dil/esp/codigo_penal_de_la_republica_argentina.pdf.

[46] J. Calles-García y P. González-Pérez, La Biblia del Footprinting, 2011.

[47] www.elhacker.net, «www.elhacker.net,» [En línea]. Available: https://www.elhacker.net/trucos_google.html.

[48] G. Sain, «Evolución histórica de los delitos informáticos,» Revista Pensamiento Penal, 2015.

[49] L. G. Segadas de Araújo, F. E. Silva Coelho y E. Kowask Bezerra, «Gestión de la Seguridad de la Información,» RENATA: Universidad Nacional de Colombia, Colombia, 2014.

[50] W. T. Jaña, «Análisis legal comparativo de la protección de datos personales a nivel Latinoamericano,» Universidad de Chile, Santiago, 2003.

[51] C. Bernadette, «Análisis del proceso de debate de iniciativas legales sobre protección de datos personales y sus conflictos con el derecho a la libertad de expresión. Los casos de Argentina y Ecuador,» Universidad de Palermo, Italia, 2021.

[52] Ministerio de Justicia y Derechos Humanos: Presidencia de la Nación, «Protección de los datos personales: Ley 25.326,» InfoLEG, Argentina, 2000.

[53] El Senado y Cámara de Diputados de la Nación Argentina, «Ley de Habeas Data: Ley de Protección de datos personales,» [En línea]. Available: https://tpc2emon09.blogspot.com/. [Último acceso: 2022].