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 peruana desde un enfoque de ciberseguridad y delitos informáticos

Autoras:

Gabriela Elizabeth Alvear Richards

Emma Alejandra Hernández Pesantes

Director:

Miguel Arturo Arcos Argudo

CUENCA – ECUADOR

2023

Autoras:

Gabriela Elizabeth Alvear Richards
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
galvear@est.ups.edu.ec

Emma Alejandra Hernández Pesantes
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
ehernandezp@est.ups.edu.ec

Dirigido por:

Miguel Arturo Arcos Argudo
Ingeniero de Sistemas.
Magíster en Seguridad de las Tecnologías de la Información y de las Telecomunicaciones.
Doctor en Ciencias de la Computación para Smart Cities.

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

DEDICATORIA

Este trabajo está dedicado, principalmente a Dios, que es mi pilar fundamental en cada etapa de mi vida.

A mi esposo Roberto Rodríguez, quien es una piedra angular en cada logro y paso que doy, gracias por su comprensión, paciencia y ánimo constante durante mis largas horas de estudio y dedicación a este proyecto.

A mi mamá Mónica Richards, por su amor incondicional, apoyo y sacrificio en cada etapa de mi vida, y en especial durante esta etapa académica que hoy concluye con éxito.

Por último, a todas las personas que aportaron en mi vida profesional y académica, a lo largo de este arduo camino.

Gabriela Alvear Richards.

Esta tesis está dedicada a mis amados padres y hermanas Emma P., Edison, Alison y Milena por su constante apoyo, aliento y amor. Su fe en mí nunca vaciló, y su constante motivación y orientación han sido fundamentales para convertirme en la persona que soy hoy. Siempre estaré agradecida por sus sacrificios, comprensión y confianza en mis habilidades.

También me gustaría dedicar este trabajo a mi amado esposo Ángel Aguilar, cuya paciencia, comprensión y apoyo constante hicieron posible que yo persiguiera mis sueños. Su fe inquebrantable en mí me dio la fuerza y la motivación para superar los desafíos que enfrenté durante este viaje. Gracias por estar a mi lado y por ser mi mayor animador.

Finalmente, dedico esta tesis a todos aquellos que me han apoyado e inspirado a lo largo de mi trayectoria académica. Su apoyo y aliento han hecho posible este logro.

Emma Hernández Pesantes.

AGRADECIMIENTO

Quiero expresar mi agradecimiento a Dios por su constante protección y guía, y por darme la fuerza y la sabiduría necesarias para alcanzar esta meta académica.

Además, deseo expresar mi más profundo agradecimiento a todas aquellas personas que de alguna manera han contribuido en la realización de este proyecto de titulación.

Agradezco a mi esposo, padres y familiares por su amor incondicional, comprensión y apoyo en cada etapa de mi vida, y en especial durante este proceso de titulación.

Agradecimiento incondicional a mi compañera y amiga de tesis Emma Hernández que sin su apoyo y compromiso no hubiéramos podido llevar a cabo este proyecto.

Quiero expresar mi gratitud a nuestro director de proyecto Miguel Arcos Argudo por su orientación, apoyo y motivación durante todo el proceso de elaboración de este proyecto. Su experiencia y sabiduría fueron fundamentales para superar los obstáculos y alcanzar los objetivos planteados.

Por último, quiero expresar mi agradecimiento a mis amigos de la Universidad, gracias por estar siempre presentes en mi vida y toda la época universitaria y mucho de ellos en este post-grado, más de 10 años conociéndonos y siendo soporte fundamental en mi crecimiento profesional y personal. Su amistad y apoyo fueron un gran aliciente en este camino.

Gabriela Alvear Richards.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a Dios por haberme dado la fuerza, determinación y perseverancia para realizar mi tesis de posgrado. Sin su apoyo y guía incondicional, no hubiera podido alcanzar mis metas.

También me gustaría extender mi más sincero agradecimiento a mi compañera de tesis Gabriela por su paciencia, dedicación y compromiso inquebrantable para llevar esta investigación hasta el final.

También agradezco a Miguel nuestro tutor de tesis por su orientación, experiencia y sabiduría a lo largo de este proceso. Su consejo y aliento nos ayudaron a superar los desafíos de este posgrado y emerger como profesionales más fuertes y capaces.

Finalmente, me gustaría agradecer a mis amigos universitarios, quienes han estado conmigo por más de una década y quienes siempre han sido una fuente de fortaleza, apoyo e inspiración. Sin su apoyo, compañerismo y amistad, esta maestría hubiera sido mucho más desafiante. Gracias a todos por su inquebrantable apoyo y aliento

Emma Hernández Pesantes.

Tabla de Contenido

Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos

AUTOR(ES):

GABRIELA ELIZABETH ALVEAR RICHARDS

EMMA ALEJANDRA HERNÁNDEZ PESANTES

Resumen

La protección adecuada de datos se ha convertido en una necesidad fundamental y riesgosa en muchos procesos personales, corporativos y gubernamentales para garantizar el uso y la protección adecuada de la información confidencial que hace parte de la vida en Internet. El 26 de mayo de 2021, entro en vigor la Ley Orgánica de Protección de Datos Personales en el Ecuador, la cual obliga a las compañías del sector público y privado que traten datos personales, a que se adecuen a sus lineamientos, bajo advertencia de aplicar sanciones que llegarían hasta el 1 % del valor de los negocios.

Este trabajo presenta un análisis comparativo de la Ley Orgánica de protección de datos Personales de Ecuador con la legislación de Perú. Se presenta una breve reseña histórica que ayudará a entender la importancia de la existencia de Leyes como esta. También se aborda la tipificación de delitos en ambos países para que se pueda entender las consecuencias de no cumplir con la Ley.

Las Leyes de Protección de Datos Personales no solo abarcan lo jurídico y organizacional, también deben cubrir los aspectos técnicos claves que puedan ayudar a garantizar la seguridad de los datos personales, es por esto que, desde una perspectiva de la seguridad de la información, se analizará recomendaciones o medidas que pueden asegurar el cumplimiento de la Ley y la tranquilidad del titular del dato personal.

Palabras clave:

Datos personales, LOPDP (Ley Orgánica de Protección de Datos Personales), LPDP (Ley de Protección de Datos Personales) , SGSI (Sistema de Gestión de Seguridad de la Información), Políticas de Seguridad

ABSTRACT

Adequate data protection has become a fundamental and risky necessity in many personal, corporate and governmental processes to ensure the proper use and protection of confidential information that is part of life on the Internet. On May 26, 2021, the Organic Law for the Protection of Personal Data came into force in Ecuador, which obliges public and private sector companies that process personal data to comply with its guidelines, under warning of applying sanctions that could reach up to 1% of the value of the business.

This paper presents a comparative analysis of the Organic Law for the Protection of Personal Data of Ecuador with the legislation of Peru. A brief historical review is presented that will help to understand the importance of the existence of laws such as this one. The typification of crimes in both countries is also discussed in order to understand the consequences of not complying with the Law.

Personal Data Protection Laws not only cover the legal and organizational aspects, they must also cover key technical aspects that can help ensure the security of personal data, which is why, from an information security perspective, we analyze the recommendations or measures that can ensure compliance with the Law and the peace of mind of the owner of the personal data.

Key Words:

Personal Data, LOPDP (Organic Law on Personal Data Protection), LPDP (Personal Data Protection Law), ISMS (Information Security Management System), Security Policies, Security Policies, etc.

1. Introducción

En la era digital, la protección de los datos personales y la privacidad de los ciudadanos se ha convertido en un tema cada vez más importante y relevante [1]. En este contexto, las leyes y regulaciones en torno a la protección de datos personales y la ciberseguridad se han convertido en una prioridad para muchos países [2]. El análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador y la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos es una tarea relevante y necesaria para evaluar y comparar el nivel de protección que ambas leyes ofrecen a los ciudadanos frente a las amenazas en línea.

Este análisis permite identificar las similitudes y diferencias entre ambas leyes en términos de definición y clasificación de los datos personales, principios y derechos de protección de datos, obligaciones de las empresas y entidades gubernamentales, medidas de seguridad que deben implementarse, y sanciones por incumplimiento, contribuye a una mejor comprensión de las leyes de protección de datos y ciberseguridad en ambos países, y ayuda a identificar posibles áreas de mejora.

Ambas leyes buscan proteger la privacidad y seguridad de la información de los ciudadanos, en un contexto en el que los delitos informáticos y la vulneración de la privacidad son una preocupación constante [3].

El motivo de este trabajo surge del deseo de investigar un campo jurídico de gran relevancia en la actualidad: la salvaguarda de los derechos de las personas frente al procesamiento automatizado de su información personal; y, su relación con el ámbito de la ciberseguridad. Esta inquietud surge debido al rápido avance de las tecnologías de la información a nivel global, lo que ha facilitado, entre otros aspectos, la transmisión de datos personales a cualquier parte del mundo, así como la creación de perfiles humanos mediante la interconexión de datos aparentemente insignificantes, entre otros aspectos relevantes [4]. Esta situación plantea un

escenario de riesgo para los derechos fundamentales de las personas, entre los cuales la privacidad es una preocupación constante. Además, es importante justificar el estudio de los sistemas legales de ambos países, lo cual se debe en gran medida a la tendencia de integración regional y al interés por la armonización de las leyes.

Para llevar a cabo esta investigación, hemos recurrido a la lectura analítica de diversas fuentes, incluyendo: textos autorizados, revistas jurídicas, otras publicaciones y la información obtenida de sitios de Internet cuyo contenido sea de calidad y publicado por fuentes oficiales o confiables.

2. Determinación del Problema

La protección de datos personales es una de las leyes más importantes de la actualidad, surgió como una estrategia de privacidad desde la década de los 1970 en países europeos [5].

Establecer una constitución no ha sido tarea sencilla en los sistemas legales. Para el caso del derecho fundamental a la autodeterminación informativa partió del inicio de debates en los que el derecho a la privacidad se consideraba insuficiente para proteger plenamente al individuo del cambio tecnológico [6].

La Ley Orgánica de Protección de Datos Personales en adelante LOPDP cambió al mundo, en la actualidad es un tema que está en boga en todos los países, sin embargo, es una respuesta al desarrollo a largo plazo en el campo de la protección de datos personales en la Unión Europea durante más de 40 años, que ha sido alentador en otras partes del mundo, incluida América Latina, en la actualidad ya son muchos los países que ya cuentan con una ley de protección de datos vigente [7].

En Ecuador, los cambios realizados a la Constitución incluyen el derecho fundamental a proteger la información personal con plenos poderes para consultar y consentir la información bajo la Constitución de 2008.

En los últimos años se ha escuchado mucho sobre el mal uso de la información de las personas sin consentimiento, lo que ha llevado a crear una ley para que esto sea normado.

Actualmente, con el desarrollo del mundo y las nuevas tendencias de digitalización y automatización, el procesamiento de datos personales por las herramientas tecnológicas va cada vez más en aumento, esto recae en la necesidad urgente de leyes, existen grandes oportunidades técnicas para recopilar, almacenar y analizar los datos, así como también salvaguardarlos. La Ley de Protección de Datos Personales permite proteger a las personas del uso de sus datos, ya sea de manera digital o física, y de amenazas, públicas o privadas [8].

Desde mayo de 2021, el Estado Ecuatoriano cuenta con su primera Ley Orgánica de Protección de Datos Personales (LOPDP), una norma destinada a garantizar la implementación del derecho a la protección de datos personales, cuyos derechos de acceso y la toma de decisiones depende de estos datos y de los tipos de datos pertinentes y de su respectiva protección. Para ello, define, previene y establece principios, derechos, obligaciones y garantías.

Actualmente, el Perú si bien fortalece el derecho de protección de datos como uno de corte constitucional, así como cuenta con leyes que exteriorizan su respectivo cumplimiento, ello todavía no es suficiente para ser validado por la Unión Europea como un país con nivel conveniente en materia de protección de datos personales como sí lo tienen Argentina y Uruguay [9].

Este trabajo se enfocará en un análisis comparativo de la legislación ecuatoriana en materia de protección de datos personales con la legislación peruana, pero también brindará recomendaciones basadas en la norma internacional ISO (Organización Internacional de Estandarización) 27001, como el conocimiento de la información o la implementación de un sistema de gestión de seguridad de datos asegura que los individuos cumplan con la protección de datos, ya que se identifica un inventario de todos los activos de información y se recomienda su manejo adecuado, incluyendo herramientas para asegurar el acceso de acuerdo a su importancia o clasificación,

además existen procedimientos para asegurar el cumplimiento de todas las leyes y reglamentos aplicables.

Algunas entidades cuentan con procesos de seguridad de la información predeterminados que impiden que se considere un sistema de gestión que permita demostrar la planificación, ejecución, verificación y actuación en caso de brechas de seguridad de la información, así que las recomendaciones se enfocarán en ayudar a trazar la ruta para dar tranquilidad en la protección de estos datos.

3. Marco teórico referencial

Los actos cometidos con el uso de las tecnologías de la información y la comunicación (TIC) son cada vez más generalizados en la sociedad, por lo que las definiciones relacionadas con el tema cobran cada vez más protagonismo para los críticos. La protección de datos personales es una de las ramas jurídicas más importantes de la actualidad. Esta ley en Ecuador está regulada de forma descentralizada, imprecisa y no informática. A continuación, revisaremos las leyes de protección de Datos de Ecuador [10].

3.1 Reseña Histórica

La historia de Internet comienza con el surgimiento de una gran fase científica en los Estados Unidos como parte de la lucha tecnológica entre los gobiernos estadounidense y soviético durante la Guerra Fría de la década de 1950. Posterior a que el gobierno soviético lanzara el satélite Sputnik en 1957, el presidente de los Estados Unidos, Dwight Einsenhower, ordenó al Pentágono que estableciera un instituto de investigación avanzada para realizar investigaciones sobre equipos militares y comunicaciones. Después del establecimiento de ARPA (Agencia de Proyectos de Investigación Avanzada, Agencia de Proyectos de Investigación Avanzada), Larry Roberts del Instituto Tecnológico de Massachusetts presentó el proyecto para crear ARPANET – Red ARPA – para la autoridad gubernamental del Departamento de Defensa, y en 1969 comenzaron las primeras pruebas de conectividad informática. Así, los científicos de la ARPANET demostraron cómo funciona el sistema, creando una red de unos 40 puntos conectados en varios lugares. ARPANET fue el motor de la investigación en este campo y ayudo a crear nuevas soluciones. En 1982, ARPANET patrocinó TCP/IP (Protocolo de control de transmisión) lo que ahora se conoce como internet [11].

La primera definición del concepto de delito informático se creó en 1983, cuando la OCDE (Organización de Cooperación y Desarrollo Económico) lo definió como

“cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos” [12].

En este caso, "Caballo de Troya" fue el nombre del primer virus a gran escala informado por IBM PC como resultado de un brote en varios estados de EE. UU. en 1984. Fueron las primeras empresas en promulgar una legislación especial para proteger los sistemas informáticos del sector público.

Así, se considera delito informático todo acto realizado a través de las TIC que afecte bienes jurídicos protegidos mediante el uso indebido de equipos informáticos. Si bien estos pueden ser aparentemente herencia, privacidad, integridad física y/o lógica de equipos informáticos y/o sitios web, implican los dos primeros y otros derechos legales protegidos por la Constitución.

A los ciberdelincuentes se los denomina “Hacker”. La palabra hacker proviene del verbo "hacker", que significa "cortar" o "cambiar" algo inusual [13]. La palabra hacker tiene un significado actual desde la década de 1950 para describir el conocimiento intelectual de ciertos dispositivos, redes sociales y diversas conexiones entre computadoras, con origen en el Instituto Tecnológico de Massachusetts, sus desarrolladores eran conocidos como “hackers”.

Podemos revisar alguna de las definiciones que tiene la palabra “Hacker”, autores como Palmer (2001) describe el término "hacker" como alguien apasionado por la programación y el estudio de los sistemas informáticos en detalle. Efectivamente, un hacker es una persona con amplios conocimientos en informática, es decir, estudia en detalle sobre sistemas operativos, programación, arquitectura informática, sistemas TIC y otras cosas más [14]. Por su lado [15] menciona que hay diferentes tipos de hackers y difieren en función de sus funciones, tales como: “White hats hacker” también conocidos como hackers blancos o sombreros blancos se caracterizan por penetrar en los sistemas informáticos y detectar errores en los mismos e informar a la empresa sobre los mismos, contribuyendo o mejorando los sistemas de seguridad informática. A veces, las empresas solicitan a estos piratas

informáticos que ingresen al sistema para descubrir vulnerabilidades y revisar o probar los sistemas de seguridad.

Los “Black Hats” (sombreros negros), conocidos como crackers, realizan funciones opuestas a las de los piratas informáticos anteriores, ya que violan los sistemas de seguridad informática, ingresan a áreas restringidas, roban y eliminan información; infectan o se apoderan de las redes, es decir, su función principal es realizar acciones maliciosas penetrando en el sistema informático para obtener una ventaja [16].

El hacking ético es un método por el cual una persona, o lo que se conoce como hacker, utiliza sus conocimientos informáticos y de seguridad para encontrar vulnerabilidades de seguridad en el sistema, con la intención de mostrárselas a la empresa para que se puede tener en cuenta. Este tipo de métodos normalmente es contratado por las empresas para asegurarse de cubrir vulnerabilidades que puedan tener los sistemas, estos contratos siempre van acompañadas de un contrato acuerdo de confidencialidad. Todas las herramientas que necesita para prevenir un desastre cibernético como el robo de identidad [17].

Gerald Wondra fue uno de los primeros condenados por delitos Informáticos, la sentencia fue de 24 meses de libertad condicional, por acceso ilícito a los sistemas de entidades financieras de Estados Unidos.

Kevin Poulsen fue sentenciado a 51 meses de prisión [18] al ser encontrado culpable de lavado de activos y obstrucción de la justicia valiéndose de medios tecnológicos.

Chris Pile fue condenado en el Reino Unido a 18 meses de prisión al ser encontrado culpable de crear y distribuir malware. Dentro de los malware creados están los virus Pathogen y Queeg que se cargan en la memoria para afectar los programas en ejecución [19].

Antes de la ley de protección de datos los delincuentes si eran procesados por ciberdelitos, sin embargo, al no existir una ley, las condenas eran muy cortas y en ocasiones no incluía cárcel.

Una de las condenas más famosas es la de Kevin Mitnick, quien fue sentenciado a 68 meses de prisión después de ser declarado culpable de escuchar llamadas telefónicas y otros cargos de fraude informático [20].

De igual forma, Albert González fue condenado a 20 años de prisión, lo que se considera una de las penas más largas para los ciberdelincuentes. Albert es el principal responsable de una de las estafas más grandes de la historia, utilizando el método de inyección SQL, robó alrededor de 170 millones de números de tarjetas de crédito y contraseñas de cajeros automáticos [21].

Ray Vision fue sentenciado a 144 meses de prisión por cargos también relacionados con el robo de información financiera: alrededor de dos millones de tarjetas de crédito. También recibió cinco años de libertad condicional y $27 millones en daños punitivos para sus víctimas [22].

Adam Botbyl fue condenado a 15 meses de prisión luego de ser declarado culpable de robar el número de tarjeta de crédito de una popular cadena de tiendas departamentales luego de obtener acceso a los sistemas de la compañía a través de una red inalámbrica. Después de obtener acceso, lo usó para modificar el código de los programas utilizados por los empleados [23].

3.2 Precisiones conceptuales

En primer lugar, abordaremos algunos términos relacionados para comprender el tema general que puedan ayudar a comprender la protección de datos personales, qué se está tratando de proteger y cómo se está tratando de proteger, es necesario entender a qué hacen referencia los países a estudiar sobre lo que se interpretará por datos personales y sobre que trata una ley orgánica.

Sobre la definición de Datos personales en el Reglamento General Europeo de Protección de Datos [24] se hace referencia que es el dato que permite identificar o hacer identificable a un individuo directa o indirectamente.

Las leyes de protección de datos de Ecuador y Perú establecen:

Ecuador

“Datos personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables: nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular”. [25]

La 1era parte de la definición es una copia literal de la definición europea. En la 2da parte, en lugar de utilizar clasificaciones generales relacionadas con la personalidad, como la identidad física o la identidad genética, los miembros de la Asamblea Nacional de Ecuador dieron ejemplos de datos personales, como números de teléfono o registros de vehículos, que pueden generar malentendidos y conflictos. de derechos

Perú

“Datos personales: Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados” [26].

La Real Academia Española establece el término “ley orgánica” como “una norma reguladora de lo protegido constitucionalmente. Derechos y libertades públicas, reconocimiento de leyes de autogobierno y sufragio universal, y demás materias previstas en la Constitución”. Su aprobación requiere una mayoría reforzada [27].

En Ecuador según la Constitución de la Republica serán leyes orgánicas:

1. Las que reglamentan la organización y funcionamiento de las instituciones creadas por la Constitución.

2. Las que regulan el ejercicio de los derechos y garantías constitucionales.

3. Las que regulen la organización, atribuciones, capacidades y funcionamiento de un gobierno autónomo descentralizado

4. De las estructuras de los partidos políticos y de los sistemas electorales y su aprobación, reforma o exención será por mayoría absoluta del 75% o de las tres cuartas partes de los miembros del Congreso.

La Ley de Protección de Datos Personales es un hito importante para el país, ya que es la primera vez que la materia es regulada por un ente regulador específico [28]. La importancia de la protección de datos hoy en día radica en que antes de la publicación de la LOPDP, solo tres países sudamericanos, incluido Ecuador, no contaban con leyes que regulen un tema de carácter técnico y registros muy complejos. El Embajador de Ecuador ante la Unión Europea, Charles-Michel Geurtse [17], señaló que la protección de datos personales es uno de los tópicos más importantes de la estrategia para la construcción de una sociedad que conozca de los sistemas de la información en Ecuador. “La puesta en marcha de la legislación de protección de datos en Ecuador se suma al esfuerzo que otros países latinoamericanos están haciendo en el marco del proceso de digitalización global en el que hoy nos encontramos, proceso en el que la Unión Europea está poniendo especial acento en la cooperación bilateral y multilateral, particularmente con los países latinoamericanos”.

3.3 Derecho a la protección de datos personales

Hay dos áreas principales en el mundo que se ocupan de la protección de datos personales. El modelo europeo “protege la información y su propiedad” [29] y busca proteger la reputación de una persona incluso después de su muerte.

La motivación de este modelo se basa en los derechos humanos individuales. El modelo americano [30] “pretende proteger la información de las personas con el concepto de privacidad”. Este derecho puede extinguirse por el fallecimiento de la persona.

Varios países han promulgado la Ley de Protección de Datos Personales y cada país está tratando de adaptarse a los conceptos básicos de dos modelos existentes de protección de datos personales a las condiciones culturales, económicas y políticas. Los siguientes son varios casos relacionados con la Ley de Protección de Datos de varios países, organizaciones y regiones del mundo.

1. Organización de las Naciones Unidas (ONU): En 1948, adoptó un documento denominado Declaración Universal de los Derechos Humanos, cuyo artículo 12 establece que las personas tienen derecho a que sus datos personales estén protegidos por la ley.
2. Alemania: La primera ley de protección de datos (Datenschutz) se adoptó en 1970. En 1977, el Bundestag alemán aprobó la ley federal Bundesdatenschutzgesetz. Esta legislación prohíbe la transferencia de datos personales sin el consentimiento del interesado.
3. Suecia: en 1973, se publicó una de las primeras leyes de protección de datos.
4. Estados Unidos: La protección de datos se basa en la Ley de Privacidad de 1974.
5. España: La ley Orgánica 15 de 1999, prevé la protección de datos personales. Esta ley fue importante para América Latina ya que sirvió de referencia para el modelo europeo.
6. América Latina. En América Latina, la legislación sobre protección de datos personales se ha vuelto necesaria debido al creciente uso de la tecnología de la información y la mayor vulnerabilidad asociada con ella. Estas leyes son casi idénticas al modelo europeo. En Argentina Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008), México (2010), Perú (2011), Colombia (2012), Ecuador (2021).

Existen incentivos económicos para que los países establezcan marcos de protección de datos personales apropiados por ley. Por ejemplo, los regímenes de protección óptimos pueden abrir mercados para inversiones internacionales y actividades comerciales que impliquen la transferencia de datos personales, lo que hace que las TIC sean más competitivos. Una normativa completa y actualizada en materia de protección de datos promueve "la confianza y la seguridad jurídica en el uso de los datos como base de los negocios y la innovación en la sociedad de la información", posibilitando así la integración tecnológica y el desarrollo económico. El establecimiento de estándares internacionales tiene costos legales, ya que no debe requerir asesoría legal para referirse a la normativa nacional respectiva y también debe evitar posibles sanciones.

Del lado empresarial donde la información es el activo más importante de una organización esta debe ser protegida de manera adecuada de las amenazas que pongan en peligro la continuidad del negocio. Para este fin existe la normativa ISO 27001 que guía en la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) el cual consiste en un conjunto de políticas, procedimientos, procesos y comprende la estructura organizativa

Con un SGSI la organización conoce los riesgos a los que se somete la información y los gestiona mediante una sistemática definida.

3.4 Reseña histórica de la Ley Orgánica de Protección de Datos de Ecuador

Ecuador, era uno de los pocos países que no contaba con una ley especializada en protección de datos personales en América Latina [31], luego de un importante retraso entre la presentación del proyecto de ley, trámite y posterior aprobación (alrededor de 20 meses), el 26 de mayo de 2021, se publica la Ley Orgánica de

Protección de Datos Personales (LOPDP) en el Registro Oficial N° 59, con vigencia a partir de esa fecha, salvo lo relativo al régimen sancionador y correctivo que entrará en vigencia a los dos (2) años de su publicación.

Este término deberá utilizarse para que los sujetos obligados por esta Ley adecuen sus prácticas a los principios establecidos en la norma y permitan el pleno ejercicio de los derechos de los titulares de los datos personales.

Antes que fuera aprobada y desarrollada la Ley Orgánica de Protección de Datos del Ecuador solo se mencionaba la protección de datos personales en ciertos artículos donde podemos mencionar las siguientes [32]:

- Constitución de la República del Ecuador – 2008 (arts. 66, 92)
- Ley Nº 162: Sistema Nacional de Registro de Datos Públicos
- Ley Nº 13: Burós de Información Crediticia (arts. 5 a 10)
- Ley Nº67: Comercio Electrónico, Firmas y Mensajes de Datos (art 9).
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley Nº 184: Especial de Telecomunicaciones (arts. 1, 14 y 39).
- Ley Orgánica de Transparencia y Acceso a la Información (LOTAIP)
- Código Orgánico Penal (COIP) (art. 178).
- Ley Orgánica de garantías jurisdiccionales y control Constitucional (arts. 49, 50, 51)
- Reglamento de clasificación de Información Reservada y Confidencial de la Defensoría Pública – 2018 (art. 2)
- Guía de tratamiento de datos personales en administración pública (art.2)

Hasta ese momento no existía una regulación clara, la protección de datos personales se encontraba dispersamente regulada en diversos cuerpos normativos, como la Constitución de la República del Ecuador, el artículo 66, la Ley Orgánica de Telecomunicaciones, el Código Orgánico Penal, entre otros. Así como también en la disposición constitucional, que contiene una cadena de unidades de protección entre ellos el “Habeas Data”, en donde también se hace referencia a los datos personales es en: “La Ley Orgánica de Telecomunicaciones en sus artículos 23 #4,

24 #14, 76, 77, 78 #2, #3 y #4; 79, 82; La Ley Orgánica de Comunicación en sus artículos 30 y 31;

El Código Orgánico Integral Penal en sus artículos 178, 180, 229 y 475; La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en sus artículos 5, 9, 48 y 49; La Ley del Sistema Nacional de Registro de Datos Públicos en sus artículos 4, 5 y 6; El Código de la Niñez y Adolescencia en su artículo 53; La Ley General de Instituciones del Sistema Financiero en su artículo 88; La Ley Orgánica de la Economía Popular y Solidaria, Art. 95; y La Ley Orgánica de Transparencia y Acceso a la Información Pública en sus artículos 2, 6 y 22".

La LOPDP se presentó como una iniciativa de proyecto luego de la noticia de la mayor filtración de datos que había ocurrido en el Ecuador y que posiblemente involucró a ex funcionarios de Gobierno (Instituciones Públicas).

En septiembre 2019. La empresa de seguridad informática vpnMentor confirmó en un informe que dos de sus especialistas descubrieron que el servidor utilizado por una empresa de análisis de datos (Novastrat) ubicado en Miami, albergaba la información personal de 20 millones de personas, la mayoría de Ecuador; este servidor no contaba con las protecciones necesarias y fue vulnerado, desencadenando esta filtración masiva con gran cantidad de información "sensible". Esa información contendría entre otros, registros del propio gobierno de Ecuador, también de una asociación de empresas automotrices y de dos bancos [32].

Al igual que este caso, en Ecuador han existido otros incidentes de filtración de datos personales de los cuales se mencionan dos a continuación:

En febrero 2021, una de las entidades financieras más grandes del Ecuador tiene problemas con una gran filtración de datos de sus usuarios. Este comunicado fue confirmado por cientos de usuarios que buscaron respuestas del banco a través de las redes sociales y anunciaron su retiro y su decisión de no usar el banco en el futuro. La entidad lo negó al principio, pero luego de unos días reconoció que hubo

un acceso no autorizado a los sistemas, que pertenecen a un proveedor que presta servicios de mercadeo del programa Pichincha Miles [33].

En Julio 2021, la ministra de Salud Pública, Ximena Garzón, corroboró en una rueda de prensa la filtración de información de 1,5 millones de personas. Entre la información sensible filtrada estaban nombres, apellidos, números de cédula, teléfonos, números de historias clínicas, diagnósticos médicos y comorbilidades de usuarios, incluidos los resultados de pruebas COVID-19, esta información estaba bajo la protección del Ministerio de Salud [34].

Sentencia. No. 2064-14-EP/21 (2021): El tribunal emitió una sentencia en la Acción Extraordinaria de Protección en la cual afirmó que la decisión de apelar la denegación de la acción de hábeas data por parte de una mujer cuyas fotos íntimas fueron reveladas sin su consentimiento, violó su derecho a tener acceso efectivo a la justicia y al debido proceso. El tribunal aseguró que se garantizará la opción inversa adecuada para la denunciante, quien ha centrado sus disputas y reclamos principalmente en aspectos relacionados con su estabilidad económica. La Corte, a través de una sentencia sustantiva, ha explicado en detalle los criterios de protección de datos personales en nuestra legislación [33] .

3.5 Reseña histórica de la Ley Orgánica de Protección de Datos de Perú

La protección de datos personales en el Perú no es nada nuevo en lo que se refiere a la regulación y la institucionalidad creada por ella. La Ley de Protección de Datos Personales, Ley 29733 – en adelante “LPDP” – data del 2011. Este fue modificado sustancialmente por el Decreto 1353 en 2017.

En el mismo año inició sus actividades la Agencia Nacional de Protección de Datos Personales (“ANPD”). Es oportuno señalar que, con anterioridad a la promulgación de la legislación de protección de datos en el Perú, ya existía normatividad del más alto nivel, no solo relacionada con este tema, sino específica sobre los derechos y protección de sus datos a nivel de entidades, el estado, etc. De hecho, en la Constitución Política del Estado, en la subsección 6 del apartado 2, se hace referencia al derecho “A que los servicios informáticos, computarizados o no, públicos o privados no suministren informaciones que afecten la intimidad personal y familiar”, a nivel constitucional, existe desde 1993 separada de la protección de los derechos relacionados con la privacidad o la intimidad; de conformidad con el artículo 200 de la Constitución, garantizando plenamente el acceso a la información permanente “procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución Política del Perú [32]".

Esto se publica, interpreta y diseña principalmente como una herramienta de acceso a la información, sujeto a la redacción de la Ley 26301 [24], “Ley de Habeas Data, de mayo de 1994, pero cuando entró en vigencia el Código Procesal Constitucional en diciembre de 2004, es que se unifica el Habeas Corpus, el Amparo, la Acción de Cumplimiento, la Acción Popular, la Acción de Inconstitucionalidad y el Habeas Data”, conocidas como acciones de garantía para proteger del derecho de “acceso” a la información incluido el derecho a conocer, actualizar, añadir, suprimir o corregir información o datos personales. La relación entre la Constitución Política del Perú y la Ley de Procedimientos Constitucionales y la Ley de Protección de Datos Personales crea puntos de contacto con otras leyes anteriormente aplicables

Otro antecedente relevante es la Ley 27489 [33], que rige desde julio de 2001 y regula la protección de los centros privados de información de riesgos y de los titulares de la información. El mensaje regula el correo electrónico comercial y está en vigor desde julio de 2005. Regula el envío de mensajes comerciales, publicitarios o promocionales no solicitados por mail y reconoce a su destinatario los siguientes derechos:

a. Sin negarse a recibir correos electrónicos;
b. Retirar su derecho a recibir (a menos que sea una condición de la oferta); servicio postal) y
c. El prestador dispone de un sistema de filtrado de correo electrónico no deseado; De acuerdo con la ley, la primera tarea era constituir un comité multisectorial encargado de redactar los decretos para controlar la acreditación de los representantes de los órganos que integran el comité y convocar a la creación del comité. El 14 de septiembre de 2011 se estableció un comité. Con una caducidad de 120 días contados a partir de la constitución de la Comisión que vencía el 7 de marzo de 2012, se registró finalmente la redacción y aprobación del Reglamento Estatutario, pero no entró en vigor hasta el año 2013.

En Perú existen varios artículos que hacen referencia a la protección de datos personales como:

- Constitución de la Republica de Peru (Art.2)
- Ley de Protección de datos Personales Ley N° 29733 (Arts. 1, 4)
- Reglamento N° 01-2020
- Código Penal del Perú (Art. 154)

3.6 Estado del Arte

Delitos informáticos: en el artículo una revisión en Latinoamérica por Gonzalez [34], expresa que se centran en los delitos informáticos en la sociedad actual, que ha adoptado las tecnologías de la información como base para gestionar sus acciones, para los autores resulta importante que con los avances tecnológicos y el impacto en el entorno de las personas, se ha terminado por adoptar actos delictivos, antes impensables y en algunos casos difíciles, previstos en la ley penal sin recurrir a aplicaciones similares prohibidas por la ley.

Es claro que en la mayoría de los países estudiados aún existen vacíos legales en algunos casos en cuanto a la regulación del uso de la información de los diferentes

medios. Si bien los gobiernos han realizado grandes esfuerzos en la lucha contra este tipo de delitos, entre ellos la piratería, la distribución de pornografía infantil, así como el uso inapropiado de información para otros fines, en conjunto; Desafortunadamente, este tipo de práctica todavía existe.

Gabi Vilca Aira [35]en su tesis de investigación sobre el Delito informático peruano hace referencia al vacío legal del Código Penal Peruano en las comunicaciones electrónicas comerciales en el cual se postulan mejoras para su regulación. Junto con el desarrollo de las tecnologías informáticas y su impacto en la mayoría de las áreas de la vida pública, se han producido una serie de actividades ilegales, comúnmente denominadas "delitos informáticos". De toda la investigación se concluye que la falta desinformación sobre los límites de las TICS es uno de los factores críticos y que impactan en la sociedad, no existe una clara definición por parte de los entes competentes sobre delito informático en dicho país.

Laura Mayer Lux [36], en su artículo de investigación publicado en junio del 2018 habla sobre los elementos criminológicos para el análisis Jurídico penal de los delitos Informáticos, el artículo analiza algunos de los factores delictivos que pueden contribuir al análisis penal de los delitos informáticos. El estudio realizado para este trabajo explora los delitos que afectan el software de los sistemas informáticos y el uso de las redes informáticas, destacando los medios y contextos de la comisión, los temas y las consecuencias, se revisa también las consecuencias de los delitos informáticos. A un nivel más granular, se sugiere que los delitos informáticos pueden tener graves consecuencias en la productividad y la economía de varias organizaciones

Para los autores del artículo Desafío de la ciberseguridad ante la legislación penal [37], los sistemas informáticos públicos en Ecuador se vieron muy afectados en 2019 después de que el gobierno ecuatoriano dejara de otorgar asilo político al Sr. Julian Assange.

Esto generó que los expertos en seguridad informática y legal participen en debates sobre aspectos importantes del delito cibernético, la seguridad cibernética, el

espacio cibernético, las leyes y regulaciones en el tratamiento de problemas relacionados con el delito cibernético. Concluyeron que una adecuada identificación de los delitos informáticos ayudaría a los abogados y autoridades competentes a evitar operaciones riesgosas que carecen del debido proceso para perseguir los delitos que utilizan medios electrónicos y se divulgan en el ciberespacio.

En la siguiente investigación se identificaron los delitos informáticos sin tipificar en nuestro Código y que el ciberdelincuente lo utiliza como vacío legal, con la finalidad de impulsar a futuro la debida regulación de leyes o dejar abierta la posibilidad a una reforma de estas.

Jonathan Endara en su artículo científico realizado en Febrero 2020 [38] habla sobre el uso de las redes sociales y su incidencia en el cometimiento de delitos contra la integridad de los niños, niñas y adolescentes, y tiene como objetivo identificar nuevas formas de comportamiento que son potencialmente dañinas para la privacidad y la dignidad, como la seducción, el acoso cibernético, los mensajes de texto sexuales y la extorsión, que es causada por el uso creciente de las redes sociales.

Es imperativo que el Estado regule estas infracciones que ocurren en Internet de manera inmediata y cuente con herramientas o mecanismos que permitan a los órganos estatales competentes garantizar los derechos en estos casos, es así, porque esa conducta es un hecho y en muchos países lo hacen gracias a la tecnología, porque las redes sociales y los avances tecnológicos son parte integral de la vida cotidiana de las personas y realizan sus actividades a través de ellas.

Diego Alejandro Cáceres, Byron Ernesto Vaca Barahona y Manuel Fernando González Puente, en su publicación del 2019 [39] hablan sobre el análisis metodológico de extracción forense en dispositivos de almacenamiento. Debido a la tecnología de dispositivos digitales, conexiones de TI, Internet y días hábiles todos los días, procesamiento de información adicional y procesamiento de datos adicionales. Cada persona tiene sus propios dispositivos, como teléfonos

inteligentes, tabletas y sus propias computadoras, muchos archivos de todo tipo de audio, videos, documentos de oficina, PDF, imágenes, etc. El análisis forense digital permite identificar paso a paso una falla o evento electrónico o informático, ya sean eventos legales como duplicación de información, acceso a bases de datos con usuario y contraseña, administrar sitios en red o en la nube. El análisis también permite reproducir eventos ilegales, como la copia no autorizada de archivos o documentos confidenciales, la piratería de bases de datos, la copia de identidades electrónicas, la piratería de servidores o dispositivos en red, y muchas otras actividades ilegales se han convertido en escenas del crimen.

Dewi Bunga en su artículo del 2019 [40] habla sobre Respuesta jurídica al cibercrimen en dimensiones mundial y nacional, detallando que el cibercrimen es un delito grave en la era de la globalización. Se utiliza tecnología sofisticada y es anónimo. Es rápido, cruza las fronteras nacionales y es impactante. El cibercrimen provoca daños materiales e inmateriales. Incluso amenaza la paz y la seguridad mundial.

Los autores [41] en su investigación del 2021 sobre el Análisis del Delito Informático en el Ecuador hace referencia a que los delitos informáticos están creciendo más rápido en América Latina en los últimos años, con pronósticos cada vez peores, de ahí la importancia y alta precisión de sus indagaciones. El estudio realizado proporciona una herramienta para entender de mejor manera el problema de los delitos informáticos desde una vista conceptual y jurídica. Los resultados experimentales muestran que existen factores como el progreso de las tecnologías de la información que inducen a un aumento bastante significativo de los delitos cibernéticos, por lo cual se requiere un análisis legal más detallado de su tipificación.

Concluye que la ley ecuatoriana es muy generalizada con respecto a los delitos informáticos, por lo que necesita ser reformada y definida para cada tipo de delito,

además de ser actualizada continuamente a fin de tomar en cuenta los cambios sociales y tecnológicos para avalar la seguridad de los usuarios de Internet.

En la investigación Los ciberdelitos y su tipificación en el Código Orgánico Integral Penal por Bélgica Castro y Diana Elizalde[42], abarcan aspectos teóricos del ciberdelito, como el perfil de los delincuentes informáticos, cómo se clasifican, cuál es el delito más común en el Ecuador, así como las bases de su legislación, llegando a la siguiente conclusión; es necesario que el estado emita un conjunto de políticas públicas para prevenir los ciberdelitos, ya que se ha demostrado que la gran mayoría de las víctimas de estos delitos caen en las trampas de los delincuentes, por lo que es necesario combatirlos con las sanciones establecidas en el Código Orgánico Penal Global, pero también requiere que el Estado, a través de sus agencias, como la Fiscalía General del Estado, tenga un mandato implementado un plan nacional para informar al público sobre los delitos cibernéticos, sus causas, sus consecuencias y cómo evitarlos.

Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador por Roxana Patricia Cedeño Villacís [43], este siglo ha traído consigo multitud de herramientas informáticas utilizadas por los ciudadanos del Ecuador en el ciberespacio, para actividades financieras, educativas, sociales y recreativas, entre otras; esto ha llamado la atención de los ciberdelincuentes.

Los delitos informáticos en Perú y la suscripción del convenio de Budapest por Marleny Yudy Huamán Cruz en el 2020 [44] surgió “por el hecho de que la delincuencia informática está más presente y por la posición que toma nuestro Estado frente a estos delitos; uno de ellos es la firma del Convenio de Budapest o Convenio sobre Ciberdelincuencia y lo que se analiza es cómo afecta la firma del citado acuerdo al tratamiento de los delitos informáticos”. La firma del Convenio de Budapest ha tenido un impacto relativo en la lucha contra los delitos informáticos, destacando la relevancia de las disposiciones del Convenio que mencionamos anteriormente, como el establecimiento de una lista de delitos penales,

el establecimiento de normas procesales para la protección de evidencia y cooperación internacional; Una característica clave es la cooperación internacional en la investigación de casos importantes, que rara vez es aplicable a partir de la fecha de la firma.

3.7 Delitos Tipificados en la LOPDP de ambos países

3.7.1 Delitos tipificados en las LOPDP de ambos países

Actualmente no existe una definición consensuada entre los abogados y la comunidad jurídica para el término “delito informático”. Sin embargo, el concepto funcional se ha desarrollado teniendo en cuenta las circunstancias específicas de cada país.

Para algunos autores, como Guibourg [45], no son más que “delitos cometidos por medios informáticos, es decir, constituyen nuevas formas de conducta ya descritas en el proceso penal, negando la existencia de bienes jurídicos autónomos a tales delitos”. En la doctrina, los delitos informáticos tienen contenido propio, afectando así nuevos intereses públicos cuyo reconocimiento legal es urgente, distinguiéndose así entre delitos informáticos, por ejemplo, nuevos tipo, y los delitos informáticos que han influido en las últimas leyes penales.

El profesor García Cantizano [46] se sumó al debate argumentando que, a pesar de que no existe una definición única de lo que constituye un delito informático en el derecho penal, cree que el delito informático puede definirse ampliamente como "el uso de sistemas automatizados de procesamiento o transmisión de datos para un propósito específico compromiso” (pp. 69-70), lo que excluye la existencia de nuevos intereses sociales. La segunda división distingue entre los dos supuestos, a saber, en primer lugar, utilizar tecnologías de la información

como un nuevo medio para influir en los derechos protegidos por la ley penal, denominados "delitos informáticos", y, en segundo lugar, tipifica los que afectan a la conducta como nuevos intereses sociales.

3.7.2 Delitos informáticos tipificados en Perú

En Perú, los delitos contra la información y los sistemas informáticos incluyen: acceso ilegal a información, atentado a la integridad de los datos informáticos y atentado a la integridad de los sistemas informáticos. Detallaremos algunos de los artículos donde se tipifican este tipo de delitos.

Artículo 36. En este artículo se clasifican las infracciones penales, las cuales son: leves, graves y muy graves, según lo determina el Decreto Ley No. 27444 en el artículo 230, artículo 4 y reconocido por el Ministerio de Justicia y Derechos Humanos. A pesar de las sanciones impuestas por las autoridades bajo su jurisdicción, podrán coordinar la implementación de una o más medidas correctivas para corregir o modificar las posibles consecuencias de la infracción o para prevenir su reincidencia.

Infracciones leves

a) Tratamientos de datos personales contrarios a las medidas de seguridad previstas en el reglamento aplicable.

b) Recopilación de datos personales, irrelevantes o insuficientes para la finalidad específica, explícita y legítima para la cual se recopilaron los datos personales.

c) No se podrá modificar o corregir los datos personales que son objeto de tratamiento si estos son inexacto o incompleto.

d) No eliminar los datos personales que son objeto de tratamiento en el momento que ya no sean necesarios, adecuados o insuficientes para la finalidad con la que fueron recogidos, o cuando haya transcurrido el plazo de tratamiento. En estos casos, no existe infracción si se ha realizado el procedimiento de anonimización o separación.

e) La no inscripción o no renovación de las actividades previstas en el artículo 34 de la Ley en el registro estatal.

f) Procesamiento de datos personales en violación de leyes y reglamentos

Infracciones graves:

a) La inobservancia, retraso o impedimento de los derechos del titular de los datos personales en los términos de la Ley n. 29733 del reglamento y el Capítulo III de su reglamento.

b) Tratamiento de datos personales, sin consentimiento libre, claro, inequívoco, previo y comunicado del titular en conformidad con la Ley n. 29733 del Reglamento de esta.

c) Tratamiento de datos personales sensibles con violación de las medidas de seguridad establecidas en los actos reglamentarios de la materia.

d) Recabar datos personales sensibles que sean innecesarios, inapropiados o insuficientes para la finalidad específica, clara y legítima para la que se requieren.

e) Utilizar los datos personales obtenidos lícitamente para fines distintos de aquellos para los que fueron recabados, salvo que existan procedimientos de anonimización o separación.

f) Impedir que la institución ejerza sus funciones de supervisión.

g) El incumplimiento del deber de confidencialidad previsto en el artículo 17 de la Ley 29733.

h) Ley n. 29733 No inscripción o no renovación de los actos señalados en el artículo 34 en el registro estatal, a pesar de las solicitudes de las instituciones dentro del proceso disciplinario.

Infracciones muy graves:

a) Tratamiento de datos personales que contravenga las obligaciones de la Ley N° 29733 y sus disposiciones, si interfiere o amenaza la realización de otros derechos fundamentales.

b) La información personal se recopila de manera fraudulenta, desleal o ilegal.

c) Proporcionar documentos o información falsa a la autoridad.

d) No se detiene el tratamiento indebido de datos personales si la institución lo ha solicitado previamente como resultado de un caso disciplinario o proceso de tutela tripartita.

e) Incumplimiento de las acciones correctivas ordenadas por la institución debido al proceso de tutela tripartita.

La cuantía de la multa dependerá de la gravedad de la infracción cometida, que será determinada por las autoridades fiscales, teniendo en cuenta las modificaciones del procedimiento penal. Perú también cuenta con la Ley no. 30096, que tiene como objetivo prevenir y sancionar las actividades ilícitas que utilicen las tecnologías de la información o la comunicación que afecten los sistemas informáticos y los datos y otros medios jurídicos relacionados con los delitos para garantizar una lucha eficaz contra el delito cibernético.

La Ley 30096(14) (Ley de Delitos Informáticos).

Ley N° 30096 "Ley de Delitos Informáticos" [47]actualizada en la ley N°30171, solo incluye delitos dolosos, lo cual quiere decir estar presente, no se admite los delitos informáticos que puedan cometerse por accidente o mala práctica, estos son llamados culpables, pero la intención debe prevalecer.

El primer artículo de la Ley de Delitos Informáticos establece que el objeto de esta ley es prever y sancionar las actividades ilícitas que afecten a los sistemas, datos informáticos, secreto de las comunicaciones; entre bienes jurídicos de trascendencia delictiva (propiedad, la opinión pública, la libertad sexual, etc.) La Ley pretende garantizar una lucha eficaz contra el ciberdelito [48].

La Ley de Delitos Informáticos consta de siete capítulos ordenados de la siguiente manera:

Capítulo 1: Objeto y Objeto de la Ley

Capítulo 2: Delitos contra los datos y sistemas informáticos.

Capítulo 3: Delitos informáticos contra la indemnización y la libertad sexual.

Capítulo 4: Delitos informáticos contra la intimidad y el secreto de las comunicaciones.

Capítulo 5: Delitos informáticos contra la propiedad.

Capítulo 6: Delitos informáticos contra la fe pública.

Capítulo 7: Normas comunes

Se menciona al margen de las modificaciones del Código Penal, los siguientes delitos:

Delitos de:

- Acceso Ilícito.
- Atentado contra la Integridad de Datos Informáticos.
- Atentado contra la Integridad de Sistemas Informáticos
- Proposiciones a menores con fines sexuales por medios Informáticos
- Interceptación de Datos Informáticos.
- Fraude Informático.
- Suplantación de Identidad mediante las TIC.
- Abuso de Mecanismos y Dispositivos Informáticos.

3.7.3 Delitos informáticos tipificados Ecuador

La evolución histórica de los ciberdelitos en Ecuador, comenzando con la Ley de Comercio Electrónico, Firmas Electrónicas y Transferencia de Datos de 2002, que tipificó como delito los delitos informáticos por primera vez en Ecuador, en el contexto de proteger el desarrollo del comercio, la educación y la cultura mediante el uso de las redes digitales y los sistemas de información, hasta el actual Código Orgánico Integral Penal (COIP), en proceso de reforma que esta ley incluyó en el anterior Código Penal, enumeró este tipo de crimen.

En la LOPDP de Ecuador no existe un apartado que tipifique los delitos como tal, sin embargo, en el Capítulo XI de la Ley menciona las medidas correctivas, infracciones y Régimen Sancionatorios.

Las infracciones establecidas en la ley son de cuatro tipos:

a) Leves del responsable

b) Graves del responsable

c) Leves del encargado

d) Graves del encargado.

Del articulo 67 al 70 detallan las infracciones de la LDPDP

"• Artículo 67 - Infracciones leves cometidas por el inspector de protección de datos.

No implementa ni mantiene las disposiciones de la Ley de Datos Personales.

• Artículo 68 - Infracciones graves del Inspector de Protección de Datos.

Se refiere a infracciones cuando no se toman las medidas adecuadas para garantizar el tratamiento de los datos personales y el mal uso de los datos declarados.

• Artículo 69 - Infracciones leves del Inspector de Protección de Datos.

Esto se refiere a la violación de la no cooperación con las personas encargadas de proteger los datos personales.

• Artículo 70 - Infracciones graves del Inspector de Protección de Datos.

Esto se aplica a los delitos resultantes del incumplimiento de la ley y el uso indebido de datos personales.

En estos artículos se detallan las infracciones por las cuales pueden ser sancionados los principales actores d esta ley; el encargado y el responsable de la protección de datos personales" [49].

Los artículos 71 a 72 prevén sanciones por infracciones a la normativa de protección de datos del 0,1% al 1% de la facturación correspondiente al volumen de negocio del ejercicio anterior a la imposición de la sanción. El volumen de negocios es el resultado de las ventas de bienes y servicios después de la deducción del IVA y otros impuestos en el ejercicio anterior.

Debido a la gran cantidad de nuevos requisitos creados por esta nueva normativa, es importante considerar el diseño para garantizar el estricto

cumplimiento de la ley, así como las prevenciones de seguridad que se deben implementar para asegurar la seguridad de la información personal

Artículo 71.- Sanciones por Infracciones leves

Determina el valor económico que se debe asumir por cometer alguna infracción.

En el mismo existe una diferencia entre funcionario público o entidad privada.

- Funcionarios públicos de 1 a 10 salarios básicos unificados
- Entidad privada en el rango 0.1% y el 0.7% según la actividad correspondiente al ejercicio fiscal anterior.

Artículo 72.- Sanciones por infracciones graves

Determina el valor económico que se debe asumir por cometer alguna infracción.

En el mismo existe una diferencia entre funcionario público o entidad privada.

- Funcionarios públicos de 10 a 20 salarios básicos unificados
- Entidad privada entre el 0.7% y el 1% sobre el negocio correspondiente al ejercicio económico anterior.

La tipificación de los delitos información reposa en el COIP, la tercera parte, de los artículos del 178 al 234, sanciona los delitos informáticos que atenten contra la seguridad de los datos confidenciales, la revelación ilícita de información, las pérdidas económicas, el acceso no autorizado, etc. [50]. (Derecho Penal para una Organización Consolidada, 2014, p. 1 93-95).

Cabe señalar que las LOPDP ecuatoriana y peruana establecen procedimientos específicos para que los titulares de datos personales ejerzan sus derechos constitucional y legalmente reconocidos, que van desde el acceso a procedimientos administrativos ante autoridades nacionales de control hasta actos de reconocimiento.

En Perú, como en Ecuador, el desconocimiento de las normas no excluye la responsabilidad. El país de Perú asume que todos sus ciudadanos conocen las

normas y leyes, por lo que pueden ser procesados como delincuentes informáticos.

La pena mínima en Perú es de menos de un año de prisión, mientras que en Ecuador es de tres años

Ambos países reclaman una exención para el tratamiento de datos personales, salvo que la ley peruana contiene disposiciones que previenen el financiamiento del terrorismo y el lavado de activos. La pena mínima en Perú es de menos de un año de prisión, mientras que en Ecuador es de tres años.

En caso de una brecha de seguridad o incumplimiento de ciertas normas legales, ambas leyes sancionan a los responsables y responsables del tratamiento de violaciones a las normas o violaciones a los derechos de datos con base en su responsabilidad frente al titular. En el caso de Ecuador se aplicarán multas entre el 0,7% y el 1% del volumen de negociación del año anterior, dependiendo de la severidad, mientras que en el caso de Perú la norma permite tres sanciones en tres niveles diferentes:

- Faltas Leves: De 0,5 a 5 UIT. Esto quiere decir que va entre los S/2.150 y S/11.500.
- Faltas Graves: De 5 a 50 UIT. Esto quiere decir que va entre los S/11.500 y S/115.000.
- Faltas Muy graves: De 50 a 100 |. Esto quiere decir que va entre los S/115.000 y S/230.000.

Las leyes ecuatorianas no cubren de manera integral el delito cibernético, por lo que deben reformarse y aclararse para cada uno de los tipos de delito y actualizarse de manera constante a medida que la sociedad y la tecnología cambian para garantizar la seguridad de los usuarios de Internet.

La LOPDP de Ecuador define algunos elementos adicionales que no están contemplados en el RGPD. Este es el marco de referencia de este impulso de la ley, aunque en algunos aspectos, como el principio de finalidad, se aplican los

mismos parámetros. Si se corresponde con la realidad sólo se podrá responder con precisión si se anuncia e implementa efectivamente el contenido previsto en la futura "Ley de Organismos de Protección de Datos Personales".

La protección de datos es una preocupación seria a nivel mundial, lo que lleva a los países latinoamericanos a adaptar su legislación. La legislación en todo el mundo, como el Reglamento General de Protección de Datos (GDPR) de la UE, enfatiza la necesidad de que los países desarrollen y actualicen sus planes y regulaciones de protección de datos actuales para que puedan adaptarse al entorno empresarial actual.

3.8 Análisis y comparación de resultados

Para esta investigación se empleó el método de análisis cualitativo, teniendo como propósito de este análisis examinar la protección de datos en Ecuador y Perú, centrándonos en la ciberseguridad y los delitos informáticos. Nuestro objetivo es evaluar las diferencias entre ambos países para recopilar la información necesaria que permita identificar posibles reformas a la ley actual de protección de datos en Ecuador.

La metodología cualitativa se fundamenta en comprender la realidad subjetiva y dinámica, que está compuesta por una multiplicidad de conceptos [54]. En el caso de este estudio, se ha utilizado la revisión bibliográfica para recopilar información relevante. Además, se ha realizado un análisis desde una perspectiva de legal, ciberseguridad y delitos informáticos en comparación con Perú. También se ha considerado los instrumentos y normas internacionales relacionados con la protección de datos. Estos enfoques y recursos han permitido obtener una comprensión más profunda y completa del tema en estudio.

Este apartado ha sido revisado por un profesional del derecho, Master Ab. Ing. Lidia Mantilla, quien cuenta con una amplia formación y experiencia en el campo del derecho y seguridad, específicamente como delegada de Protección de Datos (DPO). Su conocimiento y criterio resultan altamente relevantes para validar el estudio presentado en esta sección.

En esta comparativa podemos iniciar mencionando que ambas leyes tienen definiciones, pero en distintas connotaciones.

En comparación con la legislación peruana, la normativa ecuatoriana de protección de datos, recientemente implementada, se distingue por tener disposiciones específicas que abordan la protección de datos desde una perspectiva legal. En su constitución, Ecuador reconoce y garantiza el derecho a la intimidad personal y familiar en su artículo 66, numeral 19, el cual describe la protección de datos de carácter personal y enfatiza la necesidad de obtener autorización previa antes de procesar cualquier tipo de información [57]. Además. En contraste con la constitución peruana, esta se limita a abordar el ámbito de la vida privada y familiar en su Artículo 2, donde establece que los servicios de información, ya sea en formato digital o no, no deben vulnerar la vida privada y deben garantizar la libre circulación de la información sin falsificación [58].

En cuanto a la legislación específica de protección de datos, Ecuador promulgó su ley de protección de datos el 26 de mayo de 2021, después de la aprobación de su proyecto de ley que se presentó el 19 de septiembre de 2019. Esta ley complementa los derechos ya establecidos en la constitución. En su Artículo 1, se establece que el objetivo de la ley de protección de datos es garantizar el ejercicio de los derechos relacionados con la protección de datos personales. Además, esta ley busca impulsar el plan de gobierno electrónico para fomentar la disponibilidad de información y protección de datos personales [59].

Por otro lado, el Artículo 2 de la ley establece ciertas limitaciones en su ámbito de aplicación. Excluye de la ley los casos en los que las personas naturales utilicen

la información para fines familiares, los datos de personas fallecidas, datos anonimizados, actividades periodísticas y editoriales, datos relacionados con la gestión de riesgos, datos utilizados para la prevención e investigación de delitos, así como los datos de identificación de personas jurídicas [60].

Al comparar la nueva normativa vigente en Ecuador con la establecida en Perú, se observa que la implementación de la normativa peruana se llevó a cabo en 2013 y complementa lo establecido en su norma suprema para garantizar el derecho a la protección de datos dentro del marco del respeto a los derechos personales. Sin embargo, esta normativa peruana no proporciona una definición clara sobre varios aspectos relacionados con el tratamiento de la información, abordándolos de manera general. Esta falta de definiciones específicas puede generar ciertos vacíos al momento de ejercer y exigir derechos relacionados con la protección de datos.

Una desventaja de la normativa de protección de datos en Perú en comparación con Ecuador es el tiempo en que entraron en vigor. En el caso de Perú, la implementación de su normativa ocurrió en 2013. En contraste, Ecuador estableció su ley de protección de datos el 26 de mayo de 2021, lo que le ha permitido corregir posibles errores y realizar ajustes durante el proceso de aplicación de la ley. Esta diferencia en el tiempo de entrada en vigor puede significar que la normativa de Ecuador ha tenido la oportunidad de beneficiarse de lecciones aprendidas y experiencias de otros países, lo que puede resultar en una legislación más actualizada y efectiva en términos de protección de datos.
En Ecuador es fundamental que el propietario de la información brinde una autorización legal para la recolección, procesamiento, distribución, difusión y documentación antes de llevar a cabo cualquier acción en relación con los datos. La violación de estas normas internas puede conllevar responsabilidades civiles y penales [57].

Los principios en Ecuador difieren de los de Perú; en particular, los principios de la legislación ecuatoriana se acercan más al Reglamento General de Protección

de Datos (RGPD). La ley ecuatoriana incorpora los principios de responsabilidad proactiva y demostrada, así como el principio de favorecer al titular de los datos. Estos principios no se encuentran contemplados en la legislación peruana.

La Ley ecuatoriana reconoce el tratamiento de datos como legítimo, mientras que la normativa peruana aborda las limitaciones y el consentimiento en relación al tratamiento de datos. Un ejemplo sería que en casos en los que una entidad pública, de acuerdo con la ley, necesite obtener información, no se requerirá el consentimiento del titular de los datos.

En el Artículo 15 de la legislación peruana se aborda el flujo transfronterizo de datos personales, estableciendo que dicha transferencia solo puede realizarse hacia un receptor que cumpla con niveles adecuados de protección. Por otro lado, la ley ecuatoriana no menciona específicamente este requisito en su capítulo sobre transferencias internacionales de datos.

En contraste con la ley ecuatoriana, la legislación peruana impone obligaciones al titular de los datos personales.

La ley peruana incorpora la figura del habeas data, mientras que en la ley ecuatoriana no se menciona explícitamente.

Tanto la ley peruana como la ecuatoriana regulan los códigos de conducta y establecen las funciones de la autoridad encargada de proteger los datos personales. En Perú, la autoridad encargada de protección de datos está regulada por el Ministerio de Justicia, mientras que, en Ecuador, la Superintendencia de Protección de Datos está establecida por el Consejo de Participación Ciudadana y Control Social (CPCSS).

Tanto la legislación peruana como la ecuatoriana establecen la creación de un registro nacional de protección de datos personales.

En materia de infracciones, la ley peruana establece tres niveles: leves, graves y muy graves, mientras que en Ecuador solo se contemplan dos niveles: leves y graves.

En ambas leyes, el límite máximo de las multas corresponde al 10% de los ingresos brutos percibidos por el infractor durante el ejercicio anterior.
Las multas en Perú se calculan en base a la Unidad Impositiva Tributaria (UIT), que en el año 2022 fue de 4,600 soles (equivalente a aproximadamente 1,200 dólares estadounidenses). Estas multas pueden llegar a representar hasta el 10% de las ganancias totales.

En cuanto a derechos se trata, la Ley 29733 del Perú (LPDP) tiene menos derechos para los titulares que la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP).
Se detallan algunas diferencia y similitudes en cuanto a los derechos:

Derechos de los titulares, la LPDP otorga a los titulares una amplia gama de derechos, incluido el derecho a acceder a sus datos personales, el derecho a corregir sus datos personales, el derecho a objetar el procesamiento de sus datos personales y el derecho a ser olvidado. La LOPDP también concede el derecho a acceder a sus datos personales, el derecho a corregir sus datos personales y el derecho a oponerse al procesamiento de sus datos personales. La LPDP también otorga a los interesados el derecho al olvido, el cual no es un derecho otorgado por la LOPDP, esta modificación a la Ley 29733 fue recientemente aprobada por el Congreso de la Republica de Perú (Proyecto de Ley 4708/2022-CR) [62].

La LPDP otorga a las personas el derecho al olvido, el cual hace referencia a que se eliminen sus datos personales en determinadas circunstancias, como cuando los datos personales ya no son necesarios para el propósito para el que fueron recopilados o cuando la persona se ha opuesto al procesamiento de sus datos personales. La LOPDP no otorga a las personas el derecho al olvido.

La legislación peruana menciona el derecho a impedir el suministro de datos, mientras que en la ley ecuatoriana este derecho se denomina el derecho a la suspensión del tratamiento de datos., en la Ley peruana menciona que los datos personales tienen derecho a bloquear su suministro, especialmente cuando afecta tus derechos básicos. No aplica a la relación entre el propietario de Banco de datos personales y responsable del tratamiento de datos personales.

El Derecho a oponerse a la toma de decisiones automatizada permite a los interesados oponerse a que sus datos personales se utilicen para tomar decisiones sobre ellos sin intervención humana, este derecho no esta especificado en la ley peruada.

En el derecho a la Portabilidad, la LOPDP otorga a las personas el derecho a obtener sus datos personales en un formato estructurado, de uso común y lectura mecánica. Esto significa que las personas pueden transferir fácilmente sus datos personales de un controlador de datos a otro. La LPDP no otorga a los particulares el derecho a la portabilidad.

Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, la LOPDP especifica como derecho que los datos sensibles o datos sobre niñas, niños y jóvenes no podrán ser tratados salvo autorización expresa del titular o de su representante legal; la LPDP hace mención del reglamento donde se dictan medidas específicas para este tipo de tratamiento.

Derecho a la educación digital, en la LOPDP se hace referencia a que las personas tienen derecho a la educación digital y al acceso, conocimiento, preparación y aprendizaje responsable sobre las Tecnologías de la información, a diferencia de Perú que tiene una Ley que regula expresamente la Teleducación comunitaria en la educación básica y superior [63].

Tanto la LPDP como la LOPDP otorgan a las personas el derecho de rectificar cualquier dato personal inexacto o incompleto que se encuentre en poder de un responsable del tratamiento. Sin embargo, la LPDP también requiere que los encargados de tratamiento notifiquen la corrección a los terceros a quienes se les hayan proporcionado los datos personales inexactos o incompletos. La LOPDP no exige a los responsables del tratamiento que notifiquen a terceros las correcciones de datos personales.

El derecho de oposición es similar tanto en la ley peruana como en la ecuatoriana. Tanto la LPDP como la LOPDP otorga a las personas físicas el derecho a oponerse al tratamiento de sus datos personales. La LPDP permite que las personas se opongan al tratamiento de sus datos personales "cuando existan motivos fundados y legítimos relativos a una concreta situación personal", mientras que la LOPDP es un poco más específica con respecto a los casos en el que el titular tiene derecho a oponerse.

En la ley peruana, el derecho al tratamiento objetivo se refiere a no ser sujeto de decisiones automatizadas basadas en perfiles, mientras que en la ley ecuatoriana se conoce como el derecho a no ser objeto de tratamiento basado en la elaboración de perfiles.

La legislación peruana incluye el derecho a ser indemnizado, mientras que la ley ecuatoriana se enfoca principalmente en sanciones administrativas y en permitir al titular presentar reclamos tanto en vía administrativa como en otras instancias judiciales, como el ámbito civil e incluso penal.

Plazos para ejercer los derechos por parte del titular.

Con respecto a los plazos de respuesta que cada Ley otorga a los titulares cuando desean ejercer su derecho a solicitar información la LPDP establece el tiempo de respuesta para las solicitudes de derecho de Rectificación, Cancelación y Oposición en 10 días hábiles. Por su parte, la solicitud de acceso tiene un plazo de respuesta de 20 días hábiles, en la LOPDP el plazo será de 15 días. Aunque a

la fecha de publicación de este artículo ya se ha cumplido el plazo para que entre en vigencia el régimen sancionatorio y Ecuador sigue sin la designación de una autoridad de protección de datos. La plataforma de la Comisión de Participación Ciudadana y Control Social ha señalado hasta el momento que está en marcha "la presentación de las ternas que podrían ser evaluadas por la Comisión Técnica" [64].

Consentimiento

En cuanto a la manifestación del consentimiento en el tratamiento de datos personales y sus categorías especiales, la ley peruana tiene el consentimiento como principio, la ley ecuatoriana lo norma como derecho especifico en el Art.8, la ley ecuatoriana establece requisitos para que el consentimiento sea válido: debe ser libre, específico, informado e inequívoco. Sin embargo, no se incluyeron los dos últimos requisitos propuestos en el Proyecto de la Ley: previo y expreso. Esto plantea una problemática, ya que, aunque se requiere un consentimiento inequívoco, la ley no define claramente cómo debe manifestarse este consentimiento. Únicamente se menciona que no debe haber dudas sobre la autorización otorgada. Esto podría generar problemas como la violación de derechos, como el derecho a la autodeterminación informativa, la protección de datos e incluso la privacidad. Además, las entidades encargadas de la recolección podrían ser sancionadas por no basar el consentimiento en un estándar más riguroso.

Por otro lado, la norma peruana en este punto establece requisitos similares a los del ordenamiento europeo. El consentimiento debe ser previo, informado, expreso e inequívoco. El reglamento a la Ley N° 29733 en Perú define el alcance de estos requisitos. El consentimiento previo debe otorgarse antes de la recolección y el tratamiento de los datos. El requisito de información implica proporcionar al titular de manera clara y precisa la información relevante sobre el tratamiento y uso de los datos. El consentimiento claro e inequívoco requiere que no haya dudas sobre su otorgamiento.

En el caso de Ecuador, los requisitos de la Ley de Protección de Datos no son lo suficientemente claros ni específicos para una correcta manifestación del consentimiento. Por lo tanto, es necesario fortalecer los conceptos o reestructurar los requisitos en un posible reglamento. Obtener un consentimiento claro e inequívoco es importante para garantizar el uso adecuado de los datos y proteger los derechos fundamentales en esta materia.

Medidas de seguridad

En relación con las medidas y controles de seguridad para garantizar la privacidad de los datos personales, en comparación con la legislación ecuatoriana, la ley peruana no proporciona tantas directrices en cuanto a las medidas de seguridad para el tratamiento de datos personales.

Es necesario destacar que en la ley ecuatoriana se especifica que debe ser resultado de un análisis de riesgos y una evaluación de impacto. La metodología utilizada debe considerar las características del tratamiento, las partes involucradas y el tipo y volumen de datos personales sujetos a procesamiento.

La ley establece la obligatoriedad de llevar a cabo una evaluación de impacto en ciertos casos, como la evaluación sistemática y exhaustiva, el tratamiento a gran escala de categorías especiales de datos o de datos personales relacionados con condenas penales, y la observación sistemática a gran escala de una zona de acceso público. Adicionalmente, en caso de producirse una violación de seguridad, se establece un plazo de tres días a partir de su detección para notificarla a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones. En algunos casos, también se debe notificar al titular de los datos tan pronto como sea posible y, a más tardar, en un plazo de 5 días.

Por su parte en la ley peruana las especificaciones de medidas de seguridad no están tan detalladas en la Ley, sin embargo, cuentan con un Reglamento [65], donde se especifican una serie de medidas de seguridad que se deben aplicar en el tratamiento de Datos personales [64].

Adicionalmente, es importante destacar que la publicación de la Directiva de Seguridad por parte de la Autoridad Nacional de Protección de Datos simplifica en gran medida el proceso de análisis de riesgos de los datos personales, dividiéndolo en 4 pasos [65]:

- Identificación de los Bancos de Datos Personales.
- Análisis de los Riesgos de Seguridad.
- Aplicación de Medidas de Seguridad.
- Seguimiento.

En la ley peruana no establecen plazos para la notificación de algún tipo de incidente de seguridad que contemplen Datos personales.

Para mejorar la legislación en materia de protección de datos en Ecuador, es importante desarrollar el reglamento correspondiente a la ley orgánica actual de protección de datos. Asimismo, se hace urgente la creación del ente gubernamental independiente encargado de supervisar posibles violaciones a los derechos de protección de datos personales. Este ente tendría la responsabilidad de monitorear y garantizar el cumplimiento de las regulaciones de protección de datos.

Aunque actualmente Ecuador aun no cuenta con un Reglamento de la Ley de Protección de Datos Personales, en el capítulo VI de la Ley se detallan una serie de artículos referente a la protección de los datos personales en aspectos de tecnologías y evaluación de riegos, así mismo hace mención del ente gubernamental que debe dictar las medidas de seguridad.

La ley ecuatoriana se centra en gran medida en establecer medidas de seguridad para proteger los derechos y es muy detallada en cuanto a las infracciones. Además, la ley ecuatoriana hace referencia a estándares internacionales para garantizar el cumplimiento de medidas adecuadas. En contraste, la ley peruana no menciona específicamente estos estándares internacionales.

3.9 Recomendaciones que considerar en un SGSI a fin de garantizar la protección de los datos personales de los ciudadanos acorde a la normativa ecuatoriana y peruana.

Para cumplir con las leyes de protección de datos, cada organización debe evaluar los riesgos de los datos personales tratados con el fin de implementar los mecanismos necesarios para protegerlos. Con este fin, las organizaciones consideran la norma ISO 27001 como la guía idónea para establecer su Sistemas de Gestión de Seguridad de la Información (SGSI). La norma ISO 27001 permite a las organizaciones certificar sus SGSI. Una empresa cuyo SGSI se encuentra certificado comunica a sus clientes, empleados y proveedores su interés en proteger su información [51]. La protección de la información significa asegurar el respeto a los tres principios de seguridad: confidencialidad, integridad y disponibilidad de la información; para lo cual debe mínimamente: contar con políticas de seguridad de la información, asegurar con controles los accesos a la organización, realizar una gestión de activos que muestre la preocupación por los sistemas de información, clasificar la información, así como también se protegerla con herramientas de transferencia, implementar medidas de seguridad para las telecomunicaciones, mantener evidencia de la gestión sobre las vulnerabilidades técnicas y el monitoreo constante de incidencias de seguridad.

Las leyes de protección de datos (LPD) de Ecuador y Perú previenen el mal uso de los datos personales, especialmente aquellos clasificados como confidenciales o privados, y tiene como objetivo garantizar y proteger su tratamiento y los derechos fundamentales. También establecen la existencia de

un responsable del tratamiento de los datos personales y un responsable de la seguridad de los datos personales, es decir, dos roles dentro de una organización quienes serán los encargados de minimizar el riesgo organizativo. Por riesgo organizativo se entiende aquel que afecta directamente a la propia estructura de la organización y a la toma de decisiones que garantice el no incumplimiento con respecto a la Ley [52].

La Ley de Protección de Datos Personales (LPDP) define medidas generales de seguridad; sin embargo, en Perú también existe la Agencia Nacional de Protección de Datos Personales (APDP) que recomienda algunas directrices para las empresas individuales u organizaciones que manejan bases de datos personales para "implementar ISO/ IEC 27001" [53]. Esta directriz brinda orientación sobre las condiciones, requisitos y medidas técnicas a tener en cuenta para cumplir con la Ley de Datos Personales (No. 10. 29733) y sus disposiciones sobre medidas de seguridad de las bases de datos personales, estas son conjuntos organizados, automatizados o no, independientemente de la forma o modo en que hayan sido creados, almacenados, organizados y accedidos [54].

Aspectos técnicos o de seguridad

Si bien las leyes de protección de datos de ambos países sugieren medidas técnicas adecuadas para asegurar el cumplimiento, no especifican medidas que garantizarían la protección y por ende el cumplimiento. Por tanto, las medidas previstas en el texto de la normativa garantizan la confidencialidad, integridad, disponibilidad y estabilidad permanentes de los sistemas y servicios de tratamiento. En cualquier caso, la organización siempre debe decidir el plan de acción y la hoja de ruta de las medidas técnicas a implementar en función del contexto y las actividades de procesamiento realizadas. A continuación, se mencionan algunas recomendaciones referentes a medidas técnicas que se deberían considerar al momento de implementar un SGSI:

- Controles técnicos de seguridad de la información.

- Continuidad de negocio y medidas de emergencia.
- Medidas para proteger el uso de herramientas de uso frecuente (por ejemplo: medidas contra spam o phishing en el correo electrónico).
- Protección del sitio.
- Crear copias de seguridad y actualizar el sistema operativo.
- Cifrado de documentos y cifrado de disco.
- Sistemas de control de acceso.
- Cortafuegos.
- Herramientas que ejecuten el análisis y control de las actividades de los usuarios al enviar información desde el lugar de trabajo al extranjero, detectando fugas de información.
- Gestión de forma centralizada de las contraseñas, el control de acceso y las sesiones
- Gestión de usuarios.
- Política de incidentes y prevención de brechas de seguridad.

Estas recomendaciones ayudan a cuidar la información de las empresas que es cada vez mayor; su correcto uso y procesamiento será útil para la toma de decisiones.

La variedad de datos que se pueden asociar con una persona es bastante grande y se puede encontrar en muchas formas diferentes, tanto físicas como digitales, debido a esto los ciberdelincuentes incrementan de manera constante sus medios para planear posibles ataques amenazando la integridad de las personas y la continuidad de las organizaciones [55]. Entonces, la implementación de un SGSI basado en la norma internacional ISO 27001 asegura que las empresas cumplan con lo dispuesto en la LOPDP debido a que [56]:

1) Todos los activos de información de la entidad serán inventariados e tratados adecuadamente, incluyendo las medidas para asegurar el acceso a los mismos, de acuerdo con su importancia o clasificación.
2) Se establecerán procedimientos para asegurar el cumplimiento de todas las leyes aplicables.

La implementación de un SGSI ayuda proteger la información, los procesos y los sistemas que los utilizan, manteniendo el nivel de competitividad, cumplimiento e imagen corporativa que son necesarios para alcanzar las metas organizacionales y asegurar beneficios económicos, además, la organización les informa de las amenazas a las que está expuestos sus datos.

3.8.1 Recomendaciones:

Todas las organizaciones procesan datos personales cuya cantidad y tipos están en constante incremento. La LPDP establece un conjunto de consideraciones que las organizaciones deben cumplir con el fin de dar un tratamiento adecuado a esta información [57]. A continuación, se propone incluir algunas recomendaciones en la implementación del SGSI con el fin de facilitar el cumplimiento de la norma:

1. Elaboración de registros de actividades de procesamiento
2. Alinear los métodos de recopilación de datos de las partes interesadas con el fin de notificarles y garantizar así su derecho a la transparencia informativa.
3. Ajustar los procedimientos de aplicación de los derechos de las partes relacionadas.
4. Realizar un análisis de riesgos
5. Revisión de medidas de seguridad para garantizar la integridad, disponibilidad y confidencialidad de los datos
6. Elaborar los procedimientos y mecanismos de actuación necesarios a la hora de denunciar una brecha de seguridad
7. Analizar necesidades y obligaciones de designar delegados de Protección de Datos.
8. Elaborar una Política de Protección de Datos Personales para la organización.
9. Elaborar un plan de respuesta a incidentes de filtración de datos.

Adicionalmente, se presentan una serie de recomendaciones que ayudarán a las organizaciones a cumplir con los requisitos legales, en cuanto a seguridad de los datos.

La organización debe considerar establecer las siguientes acciones:

- Es necesario realizar la clasificación y etiquetado de los activos internos de datos, además de identificar los datos personales presentes en ellos.
- Tratar la información a lo largo de todo su ciclo de vida:
    - Durante la fase de creación de datos, es importante proteger los servicios web o sistemas utilizados para adquirir información, así como establecer un proceso seguro para adquirir dicha información.
    - En la etapa de modificación de datos, se debe controlar el acceso a la información, asegurando la protección de los activos de información. También es fundamental establecer un proceso efectivo para llevar a cabo modificaciones en la información de manera segura
    - En la fase de transmisión, se recomienda utilizar protocolos de comunicación seguros como TLSv1.1 y TLSv1.2, evitar el uso de comunicación en texto plano y aplicar controles para prevenir la fuga de información mediante soluciones como DLP (Prevención de Pérdida de Datos) y CASB (Cloud Access Security Broker).
    - En cuanto al almacenamiento de datos, se sugiere encriptar los discos y utilizar protocolos de encriptación como AES y RSA. También se menciona el enmascaramiento dinámico de bases de datos, la protección antivirus a nivel de endpoints, consideraciones para realizar copias de seguridad de la información y establecer un proceso seguro de almacenamiento de datos.
    - Para la eliminación de información, se recomienda realizar una eliminación a bajo nivel mediante métodos de borrado seguro.

Además, se deben establecer procesos adecuados para la eliminación segura de la información.

Otros aspectos importantes son la implementación de una política de clasificación de la información, un proceso de clasificación de información efectivo y una política para el tratamiento de información con terceros.
Es importante que los documentos abarquen todas las etapas del ciclo de vida de los datos, incluyendo su creación, modificación, transmisión, almacenamiento y eliminación. La documentación puede ser desarrollada a través de un análisis de riesgos que evalúe la clasificación de la información.

Esta serie de recomendaciones generan mayor confianza a las organizaciones por parte de los clientes, dado que da transparencia y seguridad en el tratamiento de los datos.

Además, existe la norma ISO/IEC 27701:2019 que sirve como guía de la gestión la privacidad de la Información la cual se recomienda implementar como extensión a la ISO/IEC 27001. Para efectos de la certificación, la gestión de privacidad de la información debe estar considerada en un SGSI, así como, recopilar la mayor cantidad de información relacionada con la empresa, identificación los activos que sean críticos y contengan datos personales.

Otras recomendaciones relacionadas con controles detallados en la norma ISO/IEC 27001 para revisar o evaluar el nivel de la protección de los datos son:

- En la etapa de planear y establecer: definir los roles y responsabilidades para cumplir con los requisitos establecidos por la ley. Es importante tener una hoja de datos para aplicar el análisis de evaluación de riesgos e identificar salvaguardas.
- En la etapa de Implementar y Operar: implementar controles para mitigar los riesgos identificados en la etapa anterior, así como, la correspondiente aceptación y comunicación de riesgos residuales.

- En la etapa de Monitorear y revisar: establecer una visión general de los controles basados en la protección de datos personales, así como su pertinencia y oportunidad, especialmente en caso de un cambio en el alcance de los requisitos físicos.
- En la etapa de mantener y mejorar: tomar decisiones para introducir cambios y mejoras a través de acciones correctivas y otro tipo de iniciativas, como la formación del personal pertinente.

Finalmente, se mencionarán una serie de recomendaciones basada en la ISO/IEC 27701 (extensión a la norma ISO/IEC 27001) que una organización puede implementar para mantener y mejorar continuamente una gestión de protección de la información dentro del SGSI adecuadamente [58]:

Sobre el contexto de la organización

- Definir el rol como controlador y/o Procesador de Datos Personales
- Determinar los factores internos y externos relevantes de su contexto y que pueden afectar su capacidad para alcanzar los objetivos de la Gestión de la Protección de la Información.
- Al momento de definir las necesidades y expectativas se debe incluir entre las partes interesadas aquellas que tienen interés o responsabilidades asociadas con el Procesamiento de los Datos Personales, incluyendo a los titulares de los Datos Personales.

La organización debe incluir en el alcance del SGSI el Procesamiento de la Protección de Datos, o extenderlo para incluirlo.

Sobre la planificación

- Incorporar en la valoración de riesgos la perdida de confidencialidad, integridad y disponibilidad de los Datos personales.
- Identificar riegos asociados al Procesamientos de Datos Personales.
- Asegurar la gestión adecuada de la relación entre la Seguridad de la Información y la protección de los Datos personas

- Evaluar las consecuencias potenciales tanto para la organización como para el titular de la Protección de Datos Personales si se materializa u riesgo de Seguridad de la Información.

Esta recomendación tiene como objetivo ayudar a la organización a cumplir con el artículo 42 de la ley, que se refiere a la evaluación de impacto en el tratamiento y protección de datos personales. Esta evaluación permitirá identificar los riesgos asociados a cada proceso y aplicar medidas de seguridad adecuadas para garantizar la protección de los datos.

Sobre las políticas de sistema de información (SI)

- Incluir el compromiso de cumplir con la legislación y requisitos contractuales aplicables a la Protección de Datos Personales.
- Considerar la legislación y requisitos contractuales aplicables a la Protección de Datos Personales.

Esta recomendación tiene como objetivo que las organizaciones establezcan políticas de seguridad que les permitan operar en cumplimiento de la ley de protección de datos personales (LODPD). Se sugiere evaluar todos los aspectos contractuales que involucren datos personales, y se recomienda la elaboración de una Política de Protección de Datos. Este documento permitirá a la organización y a su órgano de gobierno establecer los fundamentos del Sistema de Gestión de Seguridad de la Información (SGSI). La política debe definir las características, alcance y objetivos del SGSI, y también demuestra el compromiso de la entidad en la implementación del sistema de gestión, incluyendo medidas de control interno que ayuden a identificar, prever y mitigar los riesgos asociados al incumplimiento de la protección de datos.

Sobre la organización del SI – Roles y Responsabilidades

- Designar un punto de contacto de los clientes respecto al procesamiento de la Protección de Datos.
- Considerar una o más personas responsables del desarrollo, implementación, mantenimiento y monitoreo del programa organizaciones de privacidad,

para asegurar el cumplimiento de todas las leyes, regulaciones y obligaciones contractuales respecto a la Protección de Datos.

- Las personas encargadas de la protección de Datos deberían:
    - Ser independientes y reportar directamente a la alta dirección.
    - Involucrarse en togas la gestiones respecto al procesamientos de Datos personales.
    - Tener una experiencia comprobada en legislaciones, regulaciones y practica de protección de datos.
    - Ser el punto de contacto con las autoridades supervisoras
    - Informar a la alta gerencia y a toda la organización de las obligaciones respecto al procesamiento de la protección de datos.
    - Asesorar respecto a la evaluación de impacto de la privacidad realizados.

Con esta recomendación se busca incorporar al delegado de Datos Personales de la organización dentro de los roles y responsabilidades de un SGSI. Este delegado, de acuerdo a la legislación, actúa como punto de contacto con el ente regulador y asume la responsabilidad del tratamiento de datos.

Sobre la seguridad de los recursos humanos.

- Definir indicadores para asegurar que haya conciencia, se debería incluir un reporte de incidentes, respaldo a las posibles consecuencias de violar las reglas de la Protección de Procesamiento de datos personales.

Esta recomendación tiene como objetivo que en los contratos de los colaboradores se incluya una cláusula que especifique de manera explícita la responsabilidad respecto a los datos personales que la organización maneja.

Sobre la gestión de activos

- El sistema de clasificación de activos debería considerar explícitamente la Protección de Datos personales como parte del esquema que se implemente.
- Se debería asegurar que las personas de la organización estén consientes de la definición de protección de datos personales y como reconocerla.

El objetivo de esto es que la organización, dentro de su plan de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), tenga en cuenta la clasificación de activos existente, pero con un enfoque específico en la protección de datos. Por ejemplo, se sugiere clasificar la información sensible de la organización de acuerdo a lo establecido por la ley. Además, se recomienda etiquetar la información para poder tener un control efectivo sobre ella y monitorear posibles filtraciones o mal uso de los datos personales.

Sobre el control de accesos

- Se debería abordar la situación de la Protección de Datos personales de los usuarios que administran u operan sistemas o Servicios que procesan Datos personales y que esta se vea comprometida
- En caso de que se provea Procesamiento de Datos personales como servicio, debería documentarse claramente las responsabilidades del responsable de los datos personales
- Se debería mantener un registro actualizado de todo los perfiles y roles autorizados para acceder a la Información de Sistemas que contengan Datos personales.
- Se deben crear usuarios personalizados (Nombre y apellido), en caso de crear usuarios genéricos deberían ensobrarse y custodiarse.

El objetivo es que las organizaciones mantengan un registro documentado de los usuarios que acceden a datos personales, con el propósito de supervisar y controlar el acceso a dicha información. Es importante destacar que este requisito ya se encuentra contemplado en un Sistema de Gestión de Seguridad de la Información (SGSI), pero se recomienda implementarlo con un enfoque centrado en el tratamiento de los datos y considerando los diferentes tipos de datos detallados en la ley, como datos sensibles, crediticios, de salud, entre otros.

Sobre la seguridad de las Operaciones

- Se debería tener una política que aborde los requisitos de respaldo, pruebas y restauración de los Datos Personales.

- Se debe asegurar que los responsables de los Datos personales estén informados de los límites del servicio de respaldo.
- Cuando sea necesario restaurar Datos personales se debería asegurar la integridad y/o identifica su inexactitud y como resolverlas.
- Se debería mantener logs de restauración de respaldos de Protección de Datos personales, que contengan como mínimo el nombre de la persona y la descripción de los Datos Personales restaurados.

El objetivo de esta medida es garantizar que, en caso de producirse un incidente relacionado con la pérdida de datos personales, la organización disponga de un sistema de respaldo que permita restaurar la base de datos. Además, los registros de actividad (logs) serán útiles para identificar si la información ha sido manipulada y ha perdido su integridad.

Sobre la seguridad de las comunicaciones – Transferencia de la Información

- Se debería asegurar que los colaboradores con acceso a Datos Personales estén sujetos a obligaciones de confidencialidad.
- Se debería asegurar con acuerdos de confidencialidad de por medio que los colaboradores y personal externos cumplan con política de procesamiento y manejo de protección de Datos personales.

Las organizaciones deben incorporar en los acuerdos de confidencialidad disposiciones que aborden asuntos relacionados con la protección de datos. De igual manera, los contratos con proveedores o terceros deben incluir una cláusula de confidencialidad y tratamiento de datos personales.

Sobre las vulnerabilidades de seguridad

Es recomendable establecer responsabilidades y protocolos para la detección y registro de vulnerabilidades en los datos personales, así como para la notificación correspondiente a las partes involucradas y a las autoridades pertinentes, teniendo en cuenta la legislación y regulaciones aplicables.

El objetivo es que las organizaciones puedan cumplir con los requisitos legales en términos de detección de vulnerabilidades y notificación de incidentes al organismo de supervisión correspondiente.

Sobre la concientización al Personal

Es necesario establecer métricas que garanticen la sensibilización, lo cual implica la inclusión de informes de incidentes, con respecto a las posibles repercusiones de infringir las normas de protección de datos personales. Es fundamental crear conciencia tanto en los empleados internos como en los clientes externos acerca de los riesgos de seguridad y su impacto. La concientización es crucial debido a que todos tienen cierta responsabilidad en la cadena de procesamiento de datos.

Esta serie de recomendaciones pretende también ser una guía para los responsables del tratamiento de datos personales en las organizaciones.

4. Conclusiones

El análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos es un tema relevante para evaluar y comparar la protección de los datos personales y la privacidad de los ciudadanos en ambos países. A través de este análisis se puede identificar los puntos en común y las diferencias entre ambas leyes, lo que permite a las empresas y entidades gubernamentales conocer sus obligaciones y responsabilidades en materia de protección de datos. Además, permite a los ciudadanos conocer sus derechos con relación a la privacidad de sus datos personales y cómo pueden ejercerlos. En última instancia, el análisis comparativo contribuye a mejorar la protección de los datos personales y la privacidad de los ciudadanos en la era digital, lo que es fundamental en la actualidad dada la creciente importancia de la tecnología y la información en nuestras vidas.

En cuanto a las similitudes, ambas legislaciones establecen principios de protección de datos personales y regulan la recolección, almacenamiento, uso y transferencia de datos personales. Además, ambas leyes contemplan la responsabilidad por el uso indebido de datos personales y establecen sanciones para los infractores.

Sin embargo, hay algunas diferencias entre ambas leyes en cuanto a la ciberseguridad y los delitos informáticos. La Ley Orgánica de Protección de Datos Personales del Ecuador no contempla explícitamente los delitos informáticos, mientras que la legislación peruana sí lo hace. La ley peruana establece sanciones específicas para los delitos informáticos, como el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones, el sabotaje y el fraude informático, entre otros.

En cuando a las recomendaciones mencionadas es de suma importancia y esencial la ejecución de un SGSI, y que este enfoque sus controles en la ley de protección de datos personales para proteger la privacidad de los ciudadanos, cumplir con las

obligaciones legales y mejorar la reputación de la organización. Seguir algunas de las recomendaciones listadas puede generar mucho valor con respecto a la protección de la información, incluso puede mejorar la reputación de la organización entre los clientes y la sociedad en general, ya que demuestra el compromiso de la organización con la protección de los datos personales y la privacidad de los ciudadanos.

Consideremos que la implementación de un Sistemas de Gestión puede ayudar a las organizaciones a cumplir con las obligaciones legales en materia de protección de datos. Las leyes de protección de datos Personales en Ecuador y Perú establecen requisitos específicos que deben cumplirse para garantizar la protección adecuada de los datos personales. Al implementar un SGSI que cumpla con los requisitos de la ley de protección de datos, las organizaciones pueden evitar sanciones y multas por incumplimiento de la ley.

Al no tener implementado un SGSI en la organización, se torna más complicado cumplir con la Ley de Protección de Datos Personales, dado que se deberán implementar en ocasiones controles desde cero, lo cual pudiese conllevar a asumir valores económicos no presupuestados.

Finalmente, tanto la Ley Orgánica de Protección de Datos Personales del Ecuador como la legislación peruana tienen principios similares en cuanto a la protección de datos personales, pero la legislación peruana establece sanciones específicas para los delitos informáticos y obligaciones expresas para las empresas acerca de implementar medidas de seguridad para proteger la información y los sistemas informáticos. La Ley Orgánica de Protección de Datos Personales del Ecuador también establece la obligación de implementar medidas de seguridad para proteger los datos personales, pero no especifica medidas específicas de ciberseguridad.

5. Trabajos citados

[1] J. Castellanos, «La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos,» *Métodos de Información,* vol. 11, nº 21, pp. 59-82, 2020.

[2] Z. Ojeda, «El derecho a la protección de datos personales desde un análisis histórico-doctrinal,» *Tla-Melaua, revista de Ciencias Sociales,* vol. 9, nº 38, pp. 58-70, 2015.

[3] L. Sánchez, A. Santos-Olmo, E. Álvarez, E. Fernández-Medina y M. Piattini, «Cumplimiento de la LOPD y los requerimientos legales de la ISO 27001 en la citación de pacientes en Hospitales,» 2011.

[4] A. Guilayn y J. Mnclús, Aspectos legales de las redes sociales, BOSCH, 2016.

[5] [En línea]. Available: https://www.uasb.edu.ec/ciberderechos/proteccion-de-datos/#:~:text=La%20protecci%C3%B3n%20de%20datos%20personales,directiva%2095%2F46%2FCE..

[6] [En línea]. Available: https://revistas.uasb.edu.ec/index.php/foro/article/view/502/2420.

[7] [En línea]. Available: https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd/.

[8] [En línea]. Available: https://procuraduria.utpl.edu.ec/sitios/documentos/NormativasPublicas/Ley%20de%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos.pdf.

[9] [En línea]. Available: https://www.enatic.org/ficheros/descargas/estudio-enatic---derecho-comparado-en-proteccion.pdf.

[10] «https://repositorio.uasb.edu.ec/handle/10644/5945,» [En línea].

[11] «chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pensamientopenal.com.ar/system/files/2015/03/doctrina40745.pdf,» [En línea].

[12] [En línea]. Available: https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/.

[13] [En línea]. Available: https://www.significados.com/hacker/.

[14] C. Palmer, Ethical hacking, IBM Systems Journal., Vol. 4 No. 3 , (2001).

[15] L. Long, Profiling hackers, USA: SANS Institute, (2012).

[16] [En línea]. Available: https://www.significados.com/hacker/.

[17] [En línea]. Available: https://www.significados.com/hacker/.

[18] [En línea]. Available: https://dusstinjcapelo.wordpress.com/2015/09/10/los-delitos-o-fraudes-informaticos/.

[19] [En línea]. Available: https://www.timetoast.com/timelines/casos-de-delitos-informaticos-0fee2e5b-ac8b-4e06-af02-

925671ad2426#:~:text=En%201995%20Chris%20Pile%20fue,programas%20que%20estuvieran%20en%20ejecuci%C3%B3n..

[20] [En línea]. Available: https://dusstinjcapelo.wordpress.com/2015/09/10/los-delitos-o-fraudes-informaticos/.

[21] [En línea]. Available: https://www.bbc.com/mundo/cultura_sociedad/2010/03/100327_1200_hacker_gonzalez_sentencia_wbm.

[22] [En línea]. Available: https://securelist.lat/max-ray-vision-recibe-la-sentencia-ms-severa-de-la-historia-de-eeuu/75911/.

[23] [En línea]. Available: https://en.wikipedia.org/wiki/Adam_Botbyl.

[24] R. G. E. d. P. d. D. Personales, 2018. [En línea].

[25] L. d. P. d. D. Personales, 2021.

[26] «Ley de Protección de Datos Personales,» 2011.

[27] «https://tesis.usat.edu.pe/handle/20.500.12423/2332,» [En línea].

[28] P. d. D. h. u. n. régimen. [En línea]. Available: https://www.coronelyperez.com/2021/07/14/proteccion-de-datos-hacia-un-nuevo-regimen/.

[29] «Web Oficial de la Unión Europea,» 2016. [En línea]. Available: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm.

[30] FINREG360. [En línea]. Available: https://finreg360.com/alerta/el-congreso-de-los-estados-unidos-publica-el-proyecto-de-ley-americana-de-privacidad-y-proteccion-de-datos/.

[31] [En línea]. Available: https://www.derechosdigitales.org/17759/dia-de-la-proteccion-de-los-datos-personales/ .

[32] C. d. l. R. d. Perú, «Congreso de la República,» 29 Diciembre 1993. [En línea]. Available: https://www.congreso.gob.pe/Docs/constitucion/constitucion/index.html.

[33] C. d. l. República, «Congreso de la República,» 2001. [En línea]. Available: https://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/27353B1562B83B96052577C1006DB777/$FILE/C.5-cp--Ley-peruana-de-proteccin-de-datos.pdf.

[34] J., J. Bermeo, E. Villacreses y J. Guerrero, «Una revisión en Latinoamérica por González,» 2018.

[35] G. L. Vilca Aira, 2018. [En línea]. Available: http://repositorio.unasam.edu.pe/handle/UNASAM/2496 .

[36] 2018. [En línea]. Available: https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext.

[37] J. E. Q. B. M. D. A. M. S. F. F. B. Frankz Alberto Carrera Calderón, 2019. [En línea].

[38] J. Endara, 2020. [En línea]. Available: http://dspace.pucesi.edu.ec/handle/11010/565.

[39] B. E. V. B. y. M. F. G. P. Diego Alejandro Caceres, 2019.

[40] 2019. [En línea]. Available: http://jurnal.unpad.ac.id/pjih/article/view/19679/10205.

[41] J. L. R. V. L. D. P. S. Marco Fernando Saltos Salgado, 2021. [En línea].

[42] D. a. e. a. Bélgica mercedes castro montoya, 2021.

[43] R. P. C. Villacis, *Revista Tecnológica Ciencia y Educación,* 2022.

[44] 2020. [En línea]. Available: https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y.

[45] R. Guibourg, Derecho, sistema y realidad, 2014.

[46] M. d. García Cantizano, Delincuencia informática en el ordenamiento jurídico penal, peruano. Lima, 2012.

[47] C. d. l. R. d. Perú, 27 09 2013. [En línea]. Available: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf.

[48] «https://castanonhyeral.blogspot.com/2018/,» [En línea].

[49] (https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf). [En línea].

[50] P. A. &. Rosero, DELITOS COMETIDOS EN EL ECUADOR La revista Lideres, 2012.

[51] [En línea]. Available: https://www.iso27000.es/sgsi.html.

[52] «https://www.finanzaspopulares.gob.ec/wpcontent/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf,» [En línea].

[53] «https://cdn.www.gob.pe/uploads/document/file/1401560/Directiva%20de%20seguridad.pdf,» [En línea].

[54] «https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf,» [En línea].

[55] «chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unad.edu.co/bitstream/handle/10596/18453/MODELO%20PARA%20LA%20IMPLEMENTACI%C3%93N%20DE%20LA%20LEY%20DE%20PROTECCI%C3%93N%20DE%20DATOS%20PERSONALES%20BASADO%20EN%20EL%20SGSI%20DE%20LA%2,» [En línea].

[56] «https://www.inforc.lat/post/sgsi-y-el-cumplimiento-lopdp,» [En línea].

[57] «https://riunet.upv.es/bitstream/handle/10251/151243/Rodr%C3%ADguez%20-%20Gu%C3%ADa%20para%20la%20evaluaci%C3%B3n%20de%20impacto%20requerida%20en%20el%20Reglamento%20Europeo%20de%20Protecci%C3%B3n%20d....pdf?sequence=1,» [En línea].

[58] «https://www.iso.org/home.html,» [En línea].

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

[60] E. U. Websites. [En línea]. Available: https://www.eeas.europa.eu/delegations/ecuador/uni%C3%B3n-europea-participa-en-seminario-internacional-sobre-protecci%C3%B3n-de-datos_en.

[61] C. Peruana, 1993. [En línea]. Available: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2203/16.pdf.

[62] «chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unimilitar.edu.co/bitstream/handle/10654/3215/VillegasCortesNestorMauricio2011.pdf?sequence=2&isAllowed=y,» [En línea].

[63] «https://riunet.upv.es/bitstream/handle/10251/151243/Rodr%C3%ADguez%20-%20Gu%C3%ADa%20para%20la%20evaluaci%C3%B3n%20de%20impacto%20requerida%20en%20el%20Reglamento%20Europeo%20de%20Protecci%C3%B3n%20d....pdf?sequence=1,» [En línea].