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 ESPAÑOLA DESDE UN ENFOQUE DE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

AUTORES:

DIEGO FRANCISCO CABEZAS MENA
GABRIELA STEFANÍA LUCAS FRANCO

DIRECTOR:

MIGUEL ARTURO ARCOS ARGUDO

CUENCA – ECUADOR
2023

Autores:

Diego Francisco Cabezas Mena.
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
dcabezasm1@est.ups.edu.ec

Gabriela Stefanía Lucas Franco.
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
glucasf@est.ups.edu.ec

Dirigido por:

Miguel Arturo Arcos Argudo.
Ingeniero de Sistemas.
Máster Universitario en Seguridad de las Tecnologías de la información y Comunicación.
Máster Universitario en Ciencias y Tecnologías de la Computación.
Doctor en Ciencias y Tecnologías de Computación para Smart Cities.
marcos@ups.edu.ec

DEDICATORIA

A la persona más fuerte, de corazón noble y virtuosa que puedo conocer: yo

A mis padres, Luisa y Alfonso, pilares fundamentales que han estado en cada proyecto que decido realizar.

A mis hermanos, por su apoyo incondicional, consejos para ser mejor cada día.

A mi tutor, Miguel Arcos, quien desde el primer momento estuvo presto a ayudarme en la maestría.

Gabriela Lucas Franco.

DEDICATORIA

Este trabajo está dedicado a:

A mi familia, mi esposa Ana Lucía Cano y a mis 2 hijas Sabrina y Samantha, quienes me apoyaron para continuar con este nuevo logro en mi vida, la misma que me ayudará a impulsar con más fuerza las destrezas y nuevas habilidades adquiridas tanto en mi labor profesional como personal.

A mis padres Mariana Mena y Segundo Olmedo, que han luchado incansablemente para inculcar su ejemplo de lucha y esfuerzo con el fin de alcanzar mis metas.

Finalmente quiero dedicar a todos mis hermanos, a mi hermana y sobrinos quienes a pesar de las adversidades siempre han estado a mi lado, compartiendo sus consejos y opiniones, alentándome a continuar con este nuevo reto.

Diego Cabezas Mena.

AGRADECIMIENTO

En primer lugar, agradezco a mis padres Luisa Franco y Alfonso Lucas, a mis hermanos Jefferson y Luis, sin el apoyo de cada uno de ellos no habría sido posible cumplir otro de mis objetivos propuestos en mi vida.

De igual manera, agradezco tanto a mi tutor PhD. Miguel Arturo Arcos Argudo por el tiempo, dedicación y la confianza que me ha brindado desde el año 2022 y a la vez, a cada uno de los docentes que compartieron sus conocimientos, consejos y experiencias durante la maestría.

También, agradezco a mi compañero Diego Cabezas, por su apoyo incondicional, quien desde un inicio de la maestría hemos trabajado juntos para obtener el título de Magister en Seguridad de la Información.

A todos muchas gracias.

Gabriela Lucas Franco.

AGRADECIMIENTO

En primer lugar, agradezco a mi esposa Lucia Cano por apoyarme e impulsarme en esta nueva etapa de aprendizaje de mi vida, por compartirme su apoyo incondicional durante el desarrollo de este postgrado, de igual forma agradezco a mis padres por haber depositado en mí la confianza de que si es posible superar las adversidades del camino y que con mucho optimismo y perseverancia todo se puedo lograr.

Agradezco a mi sobrina Cristina Toledo, quien durante los primeros meses de estudio me supo brindar su conocimiento para culminar aquellas tareas en la cuales se presentaban algunos obstáculos y requerían de un apoyo adicional.

También estoy muy agradecido a mi tutor PhD. Miguel Arturo Arcos Argudo, por haberme entregado la oportunidad de realizar este trabajo con su guía, consejos y lineamientos he logrado efectuar este trabajo de titulación.

Por último, agradezco a los docentes que impartieron los distintos módulos compartiendo su conocimiento, experiencia profesional y sobre todo la guía en los retos para culminar cada uno de ellos.

Diego Cabezas Mena.

Tabla de Contenido

Análisis comparativo de la ley orgánica de datos personales del ecuador con la legislación española desde un enfoque de ciberseguridad y delitos informáticos

Autores:

Diego Francisco Cabezas Mena.

Gabriela Stefanía Lucas Franco.

Resumen

Con el aumento de los ciberdelitos, los países se vieron en la necesidad de crear normas y reglamentos que permitan de cierto modo evitar y reducir los delitos informáticos, los mismos que se han convertido en objetivo de los ciberdelincuentes, debido a esto, cada país establece su propia ley que garantice la protección de los datos personales de los ciudadanos identificando las diferencias en cuanto a la estructuración de cada ley y particularmente poner más énfasis en la distinción de cómo cada país tipifica y caracteriza los delitos informáticos según sus legislaciones.

Con el resultado de la comparativa se propone una serie de recomendaciones que pueden ser consideradas al momento de plantear o desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar la correcta seguridad de los datos personales de los ciudadanos en ambos países.

Palabras clave:
Código Integral Penal, Sistema de gestión de la seguridad, ciberdelito, Ley de protección, delito

ABSTRACT

With the increase in cybercrime, countries have found it necessary to create rules and regulations to prevent and reduce computer crimes, which have become the target of cybercriminals, because of this, each country establishes its own law to ensure the protection of personal data of citizens, identifying the differences in the structuring of each law and particularly put more emphasis on the distinction of how each country typifies and characterizes computer crimes according to their legislation.

With the result of the comparison, a series of recommendations are proposed that can be considered when planning or developing an Information Security Management System (ISMS) to guarantee the correct security of citizens' personal data in both countries.

Palabras clave:
Comprehensive Criminal Code, Security Management System, cybercrime, protection law, crime.

1. Introducción

Las acciones ilegales en la informática y la seguridad se remontan a inicios de 1970, con la aparición de la Internet y el paso del tiempo, su uso se incrementó en conjunto con la implementación de las Tecnologías de la Información y la Comunicación (TIC) (Bdr Informática y Comunicaciones, 2020), es ahí donde la ciberseguridad toma un rol importante dentro de las organizaciones como medida de protección ante los delitos informáticos (Universidad de Almeria, 2020).

El término delito informático, delito cibernético o también llamado ciberdelito (Wikidat, s.f.) ha ido evolucionando de la mano de la tecnología junto con el desarrollo de la sociedad (José Zambrano, 2016), incrementando los ataques producidos desde cualquier parte del planeta por medio del uso de las redes con el único fin de recopilar datos de forma no autorizada (Loredo, 2013).

El primer caso considerado como delito informático ocurrió en el año 1971, el "inocente" virus Creeper se encargaba de infectar la máquina, mostraba un mensaje que traducido decía "Atrápeme si puedes", imprimía un archivo y pasaba a otro ordenador conectado a la red, desapareciendo del anterior (Castillo, 2021).

Según el Centro Criptológico Nacional de España (CCN), el término ciberseguridad puede definirse como el conjunto de controles y acciones orientadas a la aseguración tanto de los sistemas y redes que forman parte del entorno tecnológico. Ciberseguridad o también llamada seguridad informática, nace de la necesidad tanto en las entidades públicas como privadas para protegerse de ataques maliciosos que comprometen el correcto funcionamiento de sus sistemas y la obtención de datos, con la finalidad de conseguir beneficios económicos (Reinares, 2020).

Con el pasar del tiempo tanto en España como en Ecuador la Internet experimentó un incremento sustancial en el tiempo de uso como en la cantidad de usuarios

conectados. Este hecho se evidenció aún más durante la época de pandemia a causa de la aparición de un virus de fácil propagación llamada SARS-CoV-2, muchas personas se vieron forzadas a cambiar sus rutinas, sean estas educativas o laborales. El uso de la Internet se ha fortalecido como medios de vital importancia en la vida diaria de las personas. En la mayoría de los hogares, Internet trajo grandes beneficios como la de estar conectados desde cualquier parte del mundo y también el riesgo de sufrir ataques informáticos (Soto, Castillo, & Barría, 2021). Dicha pandemia obligó a las personas a abandonar la modalidad presencial de sus actividades y a ocupar más los espacios virtuales que facilitaron de alguna manera a que el mundo no detenga del todo su productividad, sin embargo, este aumento de actividad cibernética también provocó un incremento del número de delitos informáticos (Yepes, 2021).

El propósito de la implementación de la protección de datos es asegurar que todos los ciudadanos tengan garantizado sus derechos en cuanto al uso o divulgación de su información considerada como privada o personal (Naranjo Martínez & Subía, 2021) además de "proteger las libertades públicas y derechos fundamentales de las personas físicas en especial su honor e integridad personal y familiar" (ACEN, 2018).

Es importante realizar este estudio con la finalidad de comparar la ley que rige tanto en Ecuador como en España estableciendo diferencias en sus tipificaciones en cuanto a la protección de datos y delitos informáticos.

2. Determinación del Problema

El uso de las herramientas tecnológicas ha permitido que las personas pasen más tiempo navegando en Internet, de igual manera el comercio electrónico cada año sigue ganando terreno al ofrecer sus servicios de pagos en línea. Frente a esto, nuestros datos se encuentran expuestos con mayor frecuencia debido a la falta de protección de los mismos, con este antecedente la Ley Orgánica de Protección de Datos Personales (LOPDP) será un gran aporte en garantizar y precautelar la seguridad de los ciudadanos para que las organizaciones resguarden la información de sus usuarios cumpliendo con todos los mecanismos de seguridad para evitar robos o filtraciones de documentos.

Con la LOPDP Quinto Suplemento Nº 459 del Registro Oficial, las entidades públicas y privadas están obligadas al cumplimiento de la normativa desde el 26 de mayo de 2021, con un plazo de dos años a partir de la fecha de su publicación, para que realicen los ajustes necesarios en su SGSI conforme lo establecido en cada uno de los artículos de acuerdo con su giro de negocio.

El propósito del análisis de ambas legislaciones es poder identificar y valorar el esfuerzo que realizaron para garantizar la protección de datos personales, determinando cuales fueron las causas que motivaron en la creación de la ley, así como las diferencias en sus tipificaciones relacionadas con los delitos informáticos ante un inminente crecimiento del uso de la tecnología basada en Internet especialmente en las áreas laborales y educativas, obteniendo una serie de conclusiones relevantes que resulten de la comparación entre las dos leyes desde una perspectiva de la ciberseguridad que permitan realizar recomendaciones al momento de elaborar un SGSI.

3. Marco Teórico Referencial

Uno de los primeros delitos se remonta en los años 60 's que, por medio de libros, obras, redacciones, etc., se empezaba a propagar desconfianza sobre la recopilación y acumulación de datos personales en las computadoras. Mediante un artículo publicado en un periódico de esa época apareció la expresión “delitos informáticos” o fechorías realizadas mediante ordenadores personales. Durante esos años, varios programadores y expertos informáticos denominados phreakers, utilizaban Bluebox o caja azul para efectuar llamadas gratuitas mediante la emisión de tonos que las compañías Bell Corporation y la American Telephone and Telegraph (AT&T) empleaban en sus comunicaciones a larga distancia, posteriormente se utilizó para operar transferencias de dinero a través de redes telefónicas alcanzando un nivel más sofisticado (Observatorio Guatemalteco de Delitos Informáticos - OGDI, 2022).

En la época de los años 70's y 80's existe un incremento en el uso del ordenador, ya sea de forma privada o personal y de uso general, donde surge la piratería informática, la extorsión, sabotaje. En los años 90's especialmente la piratería aprovecha la industria de películas y música. De esta forma, el avance tecnológico y el desarrollo incremental de la Internet originó nuevos métodos para mercantilizar contenidos ilícitos, entre los que se encuentran: la xenofobia, pornografía infantil, el racismo e inclusive acciones contra la seguridad del gobierno mediante la extorsión cibernética (Saltos, Robalino, & Pazmiño, 2021).

En 1994, Kevin Poulsen fue acusado por lavado de dinero y por obstaculizar la justicia empleando herramientas tecnológicas, ganando la reputación de ser uno de los principales autores de cometer delitos informáticos. Al siguiente año, Chris Pile enfrentó cargos penales al crear y distribuir los virus Pathogen y Queeg, con la finalidad de atacar a los programas que se encontraban ejecutándose. En el año 1999, Kevin Mitnick fue condenado por interceptar comunicaciones y por fraude, estos casos redefinieron el término hacker (Gutiérrez, 2013).

Flores señala que los hackers son considerados como personas que atacan la información, manipulando las tecnologías para horrorizar y robar dentro de varias plataformas a los consumidores de Internet (Flores, 2018). Por otro lado, Stallman define el término hacker como un sujeto que "explora los límites de lo que es posible, con una actitud inteligente y juguetona" (Stallman, 2009), mientras que, Salcedo et al. (Salcedo, Fernández, & Catellanos, 2012) afirma que un hacker ético es una persona apasionada en indagar los datos de los sistemas programables, además de investigar como ampliar su funcionalidad, son los encargados de crear herramientas, sistemas y lenguajes de programación facilitando la interacción con los recursos informáticos (Himanen, 2001).

En 1998, durante dos años los hackers atacaron a los usuarios robando sus datos y contraseñas procedentes de los ordenadores del Pentágono, la Administración Nacional de Aeronáutica y el Espacio (NASA), Universidades y Centros de investigación de América del norte, apoderándose de más de 3.000 documentos del departamento de energía de gran importancia (Lejarza, 2014).

El 25 de noviembre de 2014 se produjo un ataque realizado por un grupo de hackers con experiencia militar y civil donde ejecutaban pruebas, perpetraban inserciones a conveniencia hasta poder tener acceso a la red de computadoras de la empresa Sony Pictures. Finalmente, el Departamento de Justicia en los Estados Unidos, responsabilizó al norcoreano Park Jin-hyuk del ataque en septiembre de 2018 (Ruiz J. , 2015).

El 23 de diciembre de 2015 el sistema de red eléctrica de Ucrania dejó sin luz a sus habitantes por más de 5 horas debido a un ataque informático siendo el primer caso documentado públicamente, los responsables utilizaron el "Spear Phishing" también conocido como estafa mediante el uso del correo electrónico, con el objetivo de implantar un malware llamado BlackEnergy3 dentro de los equipos informáticos basándose en el uso de Excel el cual permitía ejecutar scripts como Macros (Galvez, 2019).

3.1 Delitos Informáticos

Se considera como delito informático a toda actividad ilegal que se ejecute por medio de dispositivos electrónicos o de computación cuyo objetivo es el robo de información delicada o personal (CARRILLO VINUEZA & CORTEZ OVIEDO, 2019)

Existen otras definiciones referentes al término “delito informático”.

La Organización para la Cooperación y el desarrollo Económico (OCDE) define este término a cualquier acto ilícito o antijurídico, que carece de ética, sin autorización consentida, relacionada con el tratamiento automático de datos y divulgación de información (Meléndez, 2018). Según la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) define que “es un número ilimitado de actos contra los principios de la seguridad de los datos o sistemas informáticos” (Fiscalía General del Estado, 2021).

3.1.1 Clasificación

Los delitos informáticos se podrían clasificar en: sabotaje, hurto, fraude, espionaje, tanto de software, servicios y accesos, tal cual se muestra en la Fig.1 (Revista Seguridad 360, 2021):

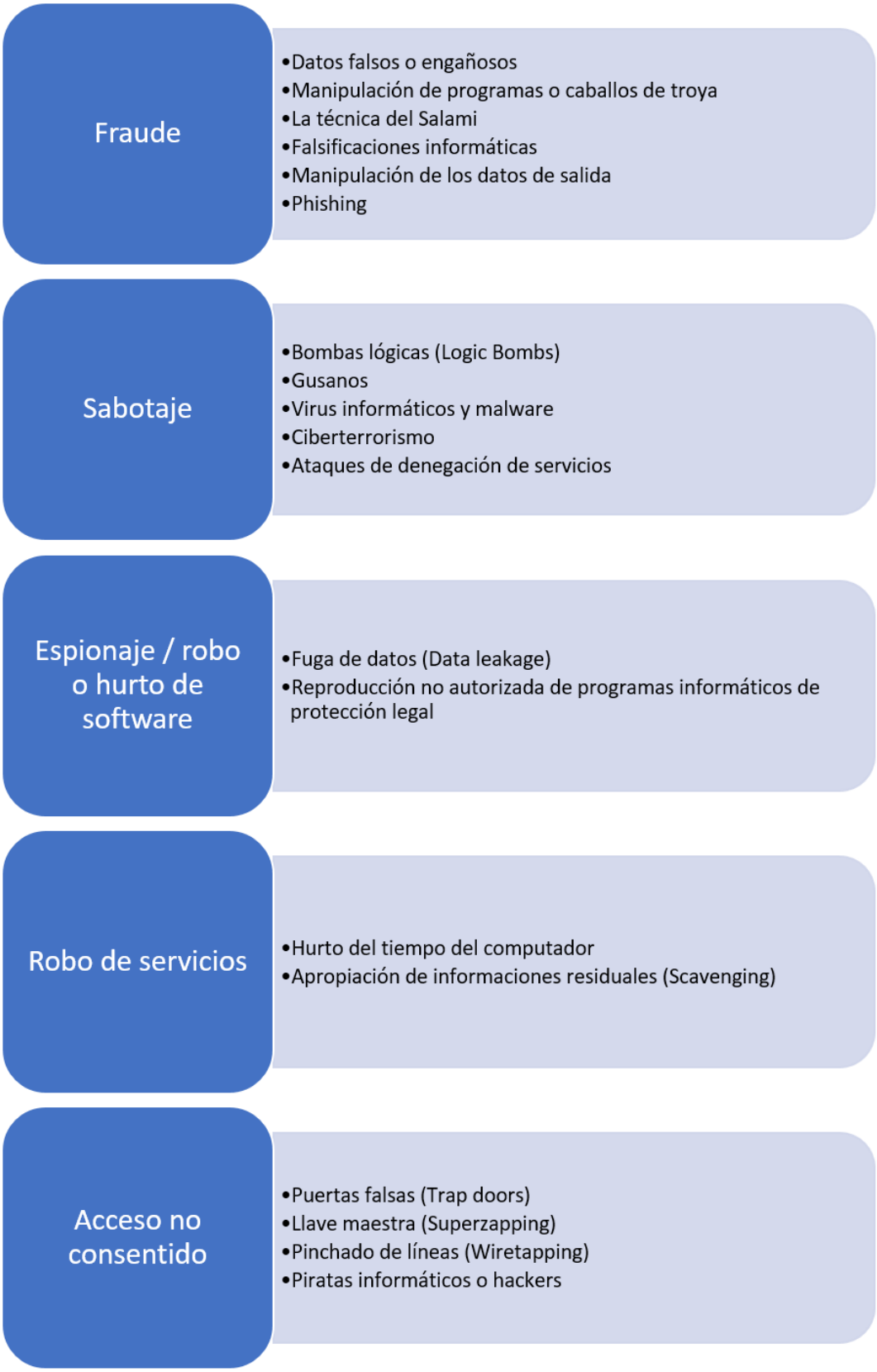

Fig. 1. Clasificación de Delitos Informáticos (Revista Seguridad 360, 2021).

3.1.2 Estadística

Las nuevas formas de conectarnos como individuos y socializar mediante el uso de la Internet, mensajes de texto o redes sociales, nos han permitido tener una comunicación más activa con otras personas en cualquier parte del mundo, esto representa una ventaja en cuanto a la comunicación, pero también se convierte en una amenaza, puesto que podríamos ser víctimas de personas mal intencionadas que buscan dañar los sistemas informáticos, robar datos personales y así obtener beneficios económicos.

A continuación, en la Fig. 2, se visualiza la comparación estadística del número de ciberataques que ambos países han enfrentado desde el año 2018 al 2020: (Statista, 2021) (TOALA, 2021).

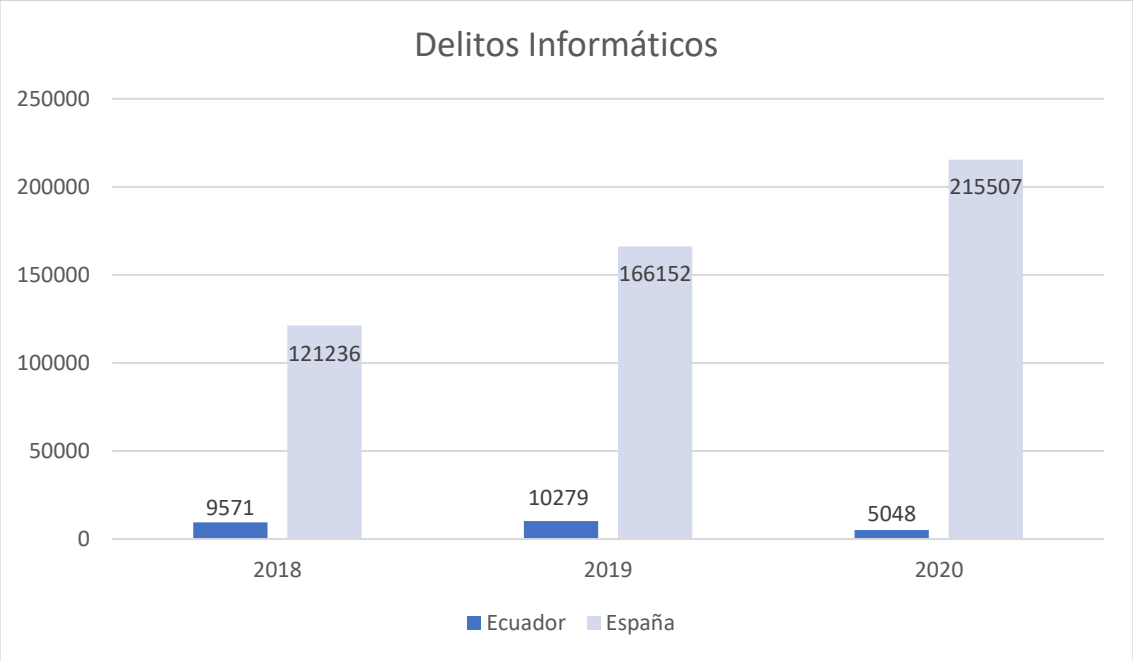

Fig. 2. Comparativa de delitos informáticos entre España y Ecuador (TOALA, 2021).

3.2 Ciberseguridad

Existen varias definiciones de ciberseguridad. De acuerdo con Cisco Systems, la ciberseguridad "es la práctica de proteger sistemas, redes y programas de ataques digitales" (CISCO, 2022). Kaspersky la define como el mecanismo de proteger ya sea

equipos, dispositivos, redes, datos y sistemas electrónicos frente a las amenazas y ataques con efecto malintencionado (Kaspersky, 2022), mientras que IBM la define como el mecanismo de proteger la información y sistemas de alta confidencialidad de los distintos ataques de forma digital (IBM, 2022).

3.2.1 Dominios

El término Ciberseguridad se aplica en diversos contextos, es por ese motivo que se clasifican en los siguientes dominios, tal como se aprecia en la Fig. 3 (Kaspersky, 2022):

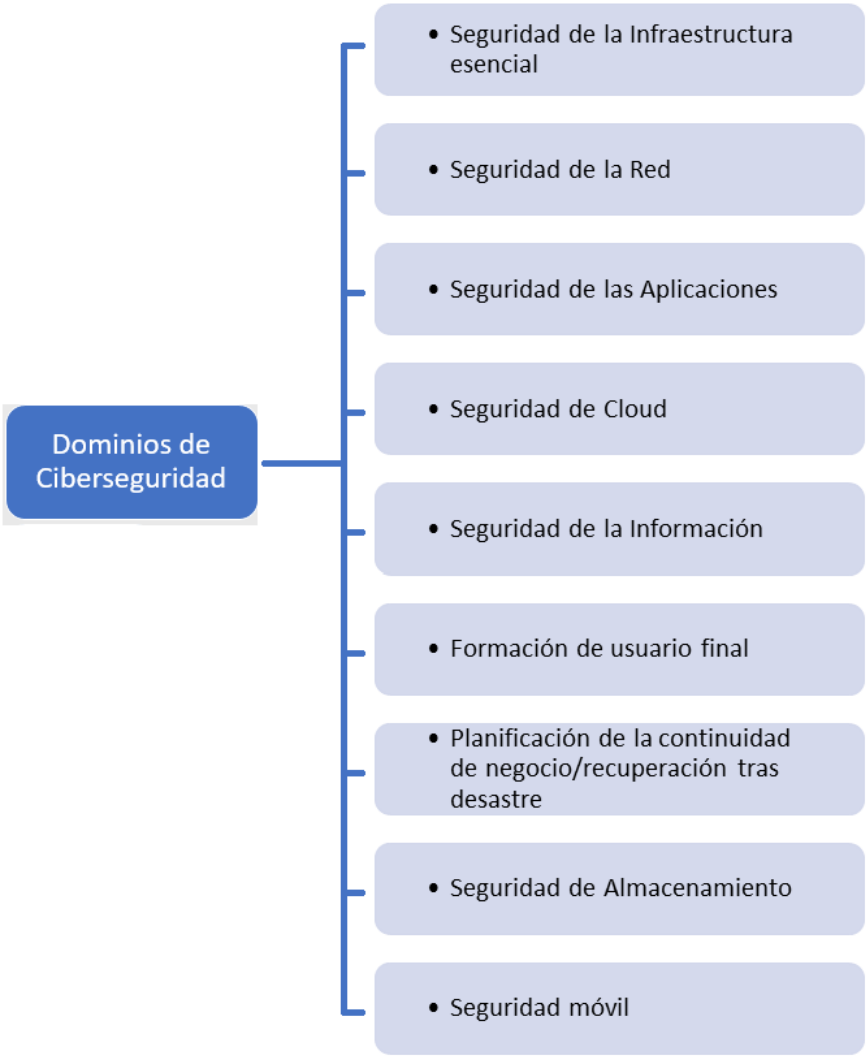

Fig. 3. Dominios de Ciberseguridad (Kaspersky, 2022)

3.3 Ley Orgánica

Una ley orgánica es aquella que posee ordenamiento jurídico para tratar en ciertos campos material de poder constitucional, para así poder regular mediante leyes ordinarias conjuntamente con la constitución de cada estado el correcto funcionamiento de las instituciones (Alzaga Villamil, 2000). Para la publicación de estas leyes, derogación o algún cambio se solicita la aprobación del poder legislativo mediante un quorum.

La Editorial Etecé, tiene una definición similar del concepto y define a una ley orgánica como aquella que da tratamiento a los asuntos importantes para la nación, normas constitucionales y libertades públicas o la articulación de los poderes del Estado, la misma que requiere de un consenso para su aprobación pudiendo ser una asamblea nacional, parlamento o congreso (Editorial Etecé, 2021).

Es necesario plantear nuevas leyes en un país cuando:

- Se necesite regular los derechos y las garantías de los ciudadanos establecidas en la constitución.
- Se precise normalizar infracciones y crear las sanciones correspondientes.
- Para imputar responsabilidades, obligaciones, competencias a los Gobiernos Autónomos Descentralizados (GAD) o a las respectivas autoridades de cada ciudad.
- Para instaurar, cambiar o derogar tributos.
- Para transformar la división político-administrativa de cada país.
- Se concede a las corporaciones públicas de control y regulación la facultad de remitir normas de carácter general (Consejo Editorial, 2015).

3.3.1 Ley Orgánica en España

El 29 de octubre de 1992, se aprobó por primera vez la ley orgánica de protección de datos personales 5/1992, tal ley tenía como centro reducir tanto el uso y técnicas de gestión de datos en forma automatizada, sobre todo los de carácter personal con el fin de garantizar el derecho al honor, proteger la intimidad y prevalecer el derecho (ALBALEGAL ABOGADOS, 2021).

Consecuentemente, en diciembre de 1999 se aprobó la Ley Orgánica 185/1999 por las Cortes Generales, optaron principalmente en regular la gestión de los datos de carácter personal en los repositorios donde estos residían, independientemente del soporte que lo respaldara; regular en una forma más detallada las labores de las personas que manipulan y tratan los datos, así como los derechos de las personas ya sean estos como encargados o responsables de los datos (ALBALEGAL ABOGADOS, 2021).

Finalmente, la Ley Orgánica 3/2018 entra en vigencia el 5 de diciembre de 2018 "Protección de Datos Personales y Garantía de los Derechos Digitales" (LOPDGDD), la misma que toma como base el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Tal ley obliga a las empresas a llevar un registro de actividades de tratamiento, en el que se incluyan carpetas con el tipo de datos recogidos y su finalidad. Hoy en día, ya no es necesario informar a la Agencia Española de Protección de Datos (AEPD) sobre dichas actividades de tratamiento (ALBALEGAL ABOGADOS, 2021).

3.3.2 Ley Orgánica en Ecuador

En Ecuador en el año 2017, la Dra. Lorena Naranjo Godoy que se desempeñaba como Directora Nacional de Registro de Datos Públicos (DINARDAP), con el apoyo de entidades públicas así como privadas, logra establecer por primera vez la Ley Orgánica de Protección de Datos Personales (LOPDP), la misma que cobraría fuerza como norma jurídica para garantizar y proteger información confidencial que son entregados a las diversas instituciones por parte de sus clientes o usuarios (Guerrón, 2021). El 19 de septiembre de 2019, en Ecuador se filtraron datos de

aproximadamente 20,8 millones de registros de ciudadanos ecuatorianos, extranjeros y fallecidos, este hecho impulsaría la publicación de la LOPDP el 26 de mayo de 2021 (Infinito Digital, 2019).

3.4 ¿Qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)?

De acuerdo con Martelo et al. (J Martelo, E Madera, & D Betín, 2015), un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas para precisar, construir, desarrollar y administrar la información de forma segura ya sea tratado en software, así como en hardware mediante la ISO/IEC 27001 SGSI; estas políticas detallan como los recursos pueden ser utilizados de forma más eficiente. El SGSI tiene un proceso de ejecución de 5 etapas que son: Implantación de políticas que aseguren la calidad y seguridad de los datos, Proyección del Sistema de Gestión, Control y análisis de riesgos, Elaboración de normas y Control de aseguramiento, mediante un modelo PHVA (Planear-Hacer-Verificar-Actuar) (HURTADO PÉREZ & ROBAYO GONZÁLEZ, 2019).

4. Materiales y Metodología

La metodología a utilizar principalmente es la revisión bibliográfica de la documentación relacionada a la Ley de protección de datos tanto de España como de Ecuador, lectura analítica y comparativa de la legislación de ambos países en donde se deberá organizar los componentes en base a una estructura de agrupación paralela, definiendo los más relevantes, encontrando las similitudes y diferencias, enfatizando entre lo positivo y lo negativo descrito en cada artículo, conociendo el ámbito de aplicación de cada una de las regularizaciones que la componen desde el enfoque de ciberseguridad y delitos informáticos, redacción sistemática de las conclusiones y recomendaciones que podrían considerarse en un SGSI de acuerdo al análisis de la normativa de cada país.

4.1 Reseña Histórica Ley de Protección de Datos

La presencia de la tecnología como parte principal del desarrollo humano ha abierto puertas para un sinfín de oportunidades tanto personales como laborales, nuestra sociedad está viviendo una época altamente conectada, la cual se facilita por medio de las TIC's, las mismas que son una parte esencial en la vida cotidiana de las personas, a tal punto que se convirtieron en herramientas indispensables y necesarias para el diario desenvolvimiento de las personas.

A lo largo del tiempo, el uso de las herramientas tecnológicas ha permitido obtener muchos beneficios al estar interconectados, sin embargo, se debe reconocer los riesgos potenciales a los que hoy en día están propensas las personas debido a su alta dependencia.

Es aquí donde se reconoce la vital importancia de mantener protegido nuestros datos que se entregan por medios digitales a los diferentes proveedores de bienes o servicios.

El uso irresponsable o en forma inadecuada de nuestros datos ha proliferado tanto que hoy en día las personas se sienten acosadas por diversos actores que obtuvieron de forma fraudulenta o sin consentimiento nuestra información.

Con este antecedente ambos países elaboraron y aprobaron una ley que permita regular y sancionar a todos los custodios de información que hagan un mal uso de los datos.

4.1.1 En España

Los inicios de la ley Orgánica que regula los datos personales en España se remontan al año de 1978. Sus principios se basan en el artículo 18.4 de la Constitución Española donde se reduce tanto el uso y técnicas de gestión de datos, con el fin de garantizar el derecho al honor, proteger la intimidad y prevalecer el derecho (Agencia Estatal Boletín Oficial del Estado, 1978),

Su evolución se ha dado de la siguiente manera:

- Ley Orgánica 5/1992 “Regulación del Tratamiento Automatizado de los Datos de Carácter Personal” (LORTAD).
- Ley Orgánica 15/1999 “Protección de Datos de Carácter Personal” (LOPD)
- Se conforma como derecho necesario para la protección de datos a cargo del Tribunal Constitucional.
- Ley Orgánica 3/2018 “Protección de datos personales y garantía de los derechos digitales” (LOPDGDD) (Villena, 2021).

4.1.2 En Ecuador

La LOPDP nace por decisión de Lenín Moreno en su calidad de presidente de la República, presentada el 19 de septiembre de 2019, luego de haber presenciado una polémica debido a la más grande filtración de información de los ciudadanos que ha ocurrido en toda la historia del Ecuador, la empresa israelí de seguridad informática vpnMentor descubrió la brecha de seguridad mientras realizaban un proyecto de mapeo a gran escala, en esta investigación se detalla que Novaestrat, compañía dedicada al análisis de datos tenía información personal de los ecuatorianos almacenada en un servidor alojado en Miami, carecía de los respectivos controles de seguridad que permitieron el acceso a los hackers y robar dicha información, este caso estaría relacionado con posibles funcionarios del Gobierno (Instituciones Públicas).

Una vez presentado el proyecto, luego de algún tiempo, este fue atendido por la Comisión de Relaciones Internacionales (RRII) y Movilidad Humana de la Asamblea Nacional, finalmente la LOPDP fue aprobada el 10 de mayo de 2021 en el pleno de la Asamblea Nacional.

Con la publicación del registro oficial, las entidades públicas y empresas privadas tenían dos años para modificar y adaptar sus procesos rigiéndose bajo los artículos de la presente ley (Social, 2021).

4.2 Delitos Tipificados Asociados a la Protección de Datos de ambos Países

En esta sección, se realiza un análisis que parte desde las infracciones en las que se pueden incurrir, así como las sanciones que aplican en cada una de ellas, adicional a esto se identifican las medidas correctivas previo a estar sujetas a los delitos tipificados.

4.2.1 Publicación o Vigencia Ley de Protección de Datos

Previo a la comparación de los delitos en función de las infracciones, sanciones y medidas correctivas es necesario partir de datos importantes tales como:

	España	**Ecuador**
Siglas	(LOPDGDD)	(LOPDP)
Nombre de la Ley	"Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales"	"Ley Orgánica de Protección de Datos Personales"
Versión \ Edición	Ley Orgánica 3/2018	Quinto Suplemento Nº 459 del Registro Oficial
Vigencia	diciembre 5, de 2018	mayo 26, de 2021

Tabla. 1. Cuadro comparativo de la publicación o vigencia de la Ley de protección de datos entre España y Ecuador.

4.2.2 Estructuración de la Ley

Información detallada de la conformación de la ley en ambos países identificando los artículos y secciones, así como las disposiciones generadas en ambas legislaciones.

Estructura	**España (LOPDGDD)**	**Ecuador (LOPD)**
Capítulos	10	12
Artículos	97	77
Disposiciones Generales	N/A	9
Disposiciones Adicionales	22	N/A
Disposiciones Transitorias	6	4
Disposiciones Reformatorias	N/A	4
Disposiciones Derogatorias	1	4
Disposiciones Finales	16	1

Tabla. 2. Comparativa de la estructura sobre la protección de datos entre España y Ecuador.

Identificación de similitudes relacionadas a la composición y estructuración de ambas leyes.

Temas	España (LOPDGDD)	Ecuador (LOPD)
Aplicación	TÍTULO I. "Medidas generales"	CAPÍTULO I: "Medios de aplicación integral"
Principios	TÍTULO II. "Principios para la protección de datos"	CAPÍTULO II: "Principios"
Derechos	TÍTULO III. "Derechos de las personas"	CAPÍTULO III: "Derechos"
Responsables / Encargados	TÍTULO V. "Responsable y encargado del tratamiento"	CAPÍTULO VII: "Responsable y delegado de la protección"
Transferencia	TÍTULO VI. "Transferencias internacionales de datos"	CAPÍTULO IX: "Transferencia o comunicación internacional de datos personales"
Tratamiento	TÍTULO IV. "Disposiciones aplicables a tratamientos concretos"	CAPÍTULO IV: "Categorías especiales de datos"
Procedimientos,	TÍTULO VIII. "Procedimientos en caso de posible vulneración de la normativa de protección de datos"	CAPÍTULO X: "De los requerimientos directos y de la gestión del procedimiento administrativo"
Autoridad	TÍTULO VII. "Autoridades de protección de datos"	CAPÍTULO XII: "Autoridad de protección de datos personales"
Infracciones, sanciones y medidas correctivas	TÍTULO IX. "Régimen sancionador"	CAPÍTULO XI: "Medidas correctivas, infracciones y régimen sancionatorio"

Tabla. 3. Comparación de estructura con relación a los temas tratados.

4.2.3 Infracciones

Para el cumplimiento de los artículos establecidos en ambas leyes, se determinan las infracciones que se pueden cometer durante la aplicación de la ley.

Tipo	Unión Europea (RGPD)	España (LOPDGDD)	Ecuador (LOPDP)
Leves	Art. 83 literal 4 y 5	Art. 74	Art. 67 y Art. 69
Graves	Art. 83 literal 4	Art. 73	Art. 68 y Art. 70
Muy graves	Art. 83 literal 5	Art. 72	NO ESTABLECIDO

Tabla. 4. Comparativa de los tipos de infracciones sobre la Protección de Datos entre: Unión Europea, España y Ecuador.

Nota: Se compara con la RGPD de la Unión Europea debido a que es la base de referencia de la LOPDGDD de España.

Infracciones leves

En Ecuador la LOPDP define para las faltas leves, el artículo 67 que aplica para el "responsable" y artículo 69 que aplica para el "encargado", ambos con la labor de proteger los datos. En comparación con Ecuador, la LOPDGDD de España define el artículo 74 que se aplica tanto para el responsable, así como para el encargado.

Infracciones graves

La LOPDP de Ecuador define para las faltas graves, el artículo 68 aplicada para el "responsable" y el artículo 70 aplicada para el "encargado" de protección de datos. En comparación con Ecuador, la LOPDGDD de España define el artículo 73 que se aplica tanto para el responsable, así como para el encargado.

Infracciones muy graves

Ecuador no define en la LOPDP artículo para las faltas muy graves mientras que, en España, la LOPDGDD define el artículo 72 que se aplica tanto para el responsable, así como para el encargado. La RGPD de la Unión Europea establece el régimen sancionador definido en el artículo 83, apartados 4, 5 y 6 empleando las disposiciones establecidas en el artículo 58.2, del literal a) hasta h) y j).

4.2.4 Multas

Ambas leyes que fueron objeto de análisis, entre las dos se pudo identificar que establecen multas o sanciones en cuanto al cometimiento de infracciones las cuales se detallan en la siguiente tabla:

Tipo	Unión Europea (RGPD)	España (LOPDGDD)	Ecuador (LOPD)
Leves	NO ESTABLECIDO	Hasta € 40.000	1 – 10 SBU o 0.1 % – 0.7 % del volumen de negocio
Graves	Multa de € 10 millones, o el pago del 2 % de la facturación anual.	Multa desde € 40.001 a € 300.000	10 – 20 SBU o 0.7 % – 1 % del volumen de negocio
Muy graves	Multa de € 20 millones, o el pago del 4 % de la facturación anual.	Multa desde € 300.001 a € 20 millones, o el pago del 4 % de la facturación anual.	NO ESTABLECIDO

Tabla. 5. Comparativa de los tipos de multas sobre la Protección de Datos entre: Unión Europea, España y Ecuador.

Las multas en España son superiores en relación con Ecuador tanto para las faltas leves y graves a excepción de las infracciones de tipo muy grave debido a que el país latinoamericano aún no tiene establecido el valor de la sanción (Grupo Atico34 , 2022).

Nota: El Salario Básico Unificado (SBU) en Ecuador es de $450 (Primicias, 2022).

A pesar de que las sanciones económicas no son tan fuertes como las establecidas en la Unión Europea considerando el volumen de la operación económica empresarial que es mucho más grande que en Ecuador, las sanciones definidas en el artículo 73 de la LOPDP están relacionadas con el margen de ventas (Ruiz M. , 2021).

4.2.5 Medidas Correctivas

Las medidas correctivas que se definen en ambas leyes tienen la finalidad de incurrir en las malas prácticas de la aplicación de la ley o inclusive que sigan cometiendo infracciones.

España (LOPDGDD)	Ecuador (LOPD)
Art. 76 El objetivo de establecer medidas correctivas es para que los actores eviten cometer estas infracciones y de igual forma que la conducta no se produzca nuevamente. Tomando como atenuante beneficios económicos obtenidos o las pérdidas evitadas.	**Art. 65 y Art. 66** Se establecen medidas correctivas para evitar cometer las mismas infracciones. Además de permitir que puedan corregir, revertir o eliminar los incumplimientos a esta ley. En caso de no cumplimiento: **Art. 66 literal 1 Leve:** Procedimiento administrativo. **Art. 66 literal 2 Grave:** Aplicación de infracciones graves y procedimiento administrativo. **Art. 66 literal 3 Muy grave:** Procedimiento administrativo
Medidas correctivas	
1) En determinadas condiciones se establece la detención del procedimiento o en algunos casos bajo condiciones de plazo. 2) Obligatoriedad al olvido mediante la eliminación de los datos. 3) La obligación de medidas técnicas, jurídicas, organizativas o administrativas para asegurar de una forma más adecuada la gestión de los datos.	1) El cese del tratamiento, bajo determinadas condiciones o plazos. 2) La eliminación de los datos. 3) La imposición de medidas técnicas, jurídicas, organizativas o administrativas a garantizar un tratamiento adecuado de datos personales.

Tabla. 6. Comparativa de las medidas correctivas sobre la Protección de Datos entre: España y Ecuador.

En la LOPDP de Ecuador en la Disposición Transitoria Primera, en la que se menciona que para las medidas correctivas de los artículos 65 y 66, además del régimen sancionatorio que entrará en vigor 2 años después a partir de la fecha de publicación, plazo con el que contarán las empresas y organizaciones para realizar ajustes a sus modelos de datos y estar alineados con las disposiciones de la ley en vigencia garantizando los principios, derechos, obligaciones y mecanismos de custodia.

De acuerdo con el artículo 76 de la LOPDGDD de España, las medidas correctivas estarán sujetas a investigación determinando circunstancias de cada caso individual, además de tomar acciones inmediatas como la sanción a los responsables, retiro de certificaciones y en el peor escenario la suspensión de los procesos. (Ruiz M. , 2021).

Tanto en LOPDGDD como en la LOPDP, se puede observar que existen 3 medidas correctivas con el mismo trasfondo, en ambas leyes tienen el objetivo de evitar que se siga cometiendo la infracción.

4.2.6 Código Penal

Parte del análisis que conforma la aplicabilidad de ambas leyes y el cometimiento de infracciones identificando los delitos tipificados que guardan relación con la seguridad de la información.

España

Los delitos informáticos tipificados en España reconocidos en el Código Penal (CP) son:

Categoría	Delito	Penalización
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	Art. 197 "Descubrimiento y revelación de secretos"	Prisión 1 – 4 años Multa 12 – 24 meses
	Art. 278.1 "Delitos relativos al mercado y a los consumidores"	Prisión 2 – 4 años Multa 12 – 24 meses
	Art. 264.1 "Daños"	Prisión de 6 meses a 3 años
Delitos informáticos	Art. 248 y 249 "Estafa"	Prisión 6 meses a 3 años
	Art. 255 y 256 "Defraudaciones de fluido eléctrico y análogas"	Multa 3 – 12 meses
Delitos relacionados con el contenido	Art. 186 "Delitos de exhibicionismo y provocación sexual"	Prisión 6 meses a 1 año Multa 12 – 24 meses
	Art. 189 "Delitos relacionados con temas sexuales como explotación, corrupción y prostitución sexual de menores"	Prisión 1 – 5 años
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.	Art. 270 "Delitos relativos a la propiedad intelectual"	Prisión 6 meses a 4 años Multa de 12 – 24 meses
	Art. 273 "Delitos relativos a la propiedad industrial"	Prisión 6 meses a 2 años Multa 12 – 24 meses

Tabla. 7. Información de los delitos informáticos y penalización según el CP español (Division Computer Forensic, 2022) .

ECUADOR

Los delitos informáticos tipificados en Ecuador recocidos en el Código Orgánico Integral Penal (COIP) son: (Asamblea Nacional del Ecuador, 2022):

Categoría	Delito	Penalización (prisión en años)
Los fraudes Informáticos	Fraude informático	3 – 5
	Recolección (Pharming) y Pesca (Phishing)	3 – 5
	"Alteración electrónica de activo patrimonial" (art. 231)	3 – 5
El sabotaje Informático	"Vulneración de sistemas informáticos" (art. 232)	3 – 5
	"Acceso no consentido a información reservada legalmente" (art. 233)	5 – 7
El espionaje informático	"Pornografía infantil" (art. 103)	13 – 16
	"Vulneración a la intimidad" (art. 178)	1 – 3
	"Interceptación de las comunicaciones o datos informáticos" (art. 476)	3 – 5
Los accesos no autorizados a sistemas de información	"Acceso sin autorización a un sistema informático, telemático o de telecomunicaciones" (art. 234)	3 – 5
	"Interceptación ilegal de datos" (art. 230)	3 – 5
	"Revelación ilegal de base de datos" (art. 229)	3 – 5

Tabla. 8. Información de los delitos informáticos y penalización en la Ley según el COIP (Ramirez, 2017).

5. Recomendaciones a considerar en un SGSI acorde a la normativa analizada

Dentro de esta sección se redacta todas las consideraciones o recomendaciones que se deben tomar en cuenta al momento de elaborar o preparar un SGSI, partiendo como línea base desde los 12 capítulos definidos en la LOPDP de Ecuador y 10 capítulos en la LOPDGDD de España en conjunto con la definición de los distintos artículos que marcan particularidades con respecto al uso, gestión y divulgación de la información.

El principal objetivo es brindar un conjunto de recomendaciones alineadas tanto con la LOPDP como de la LOPDGDD para poder generar todas las políticas necesarias durante la preparación de un SGSI.

Considerar que, según el informe “Estado actual de la Ciberseguridad en Ecuador” presentado por la empresa Deloitte y publicado en la revista IT ahora en junio de 2022, menciona que el 6% de las organizaciones cuentan con un SGSI formal, en cambio el 47% cuentan con un SGSI pero sin certificar, basándose en la normativa o delitos informáticos tipificados en la ley acorde al COIP (Deloitte, 2020).

Con la vigencia de la LOPDP, dichas organizaciones deberán realizar cambios en sus SGSI para cubrir en su totalidad las normas vigentes dispuestas en los distintos artículos de la nueva ley.

Las organizaciones como entes responsables deberán establecer políticas y controles durante la elaboración de un SGSI tomando como base la LOPDGDD y todas sus disposiciones que actualmente se encuentran vigentes.

Recomendaciones para un SGSI España

Para la elaboración de un SGSI alineados con la normativa de LOPDGDD, se deben considerar las siguientes recomendaciones:

- Para dar un buen uso y gestión de la información se debe establecer las respectivas medidas necesarias en función de la LOPDGDD con el propósito de mitigar incidentes de seguridad y tomando en consideración los distintos niveles de riesgos.
- En las organizaciones es necesario crear perfiles para cada trabajador en función al cargo que desempeña en la empresa con el fin de restringir el acceso a personas no autorizadas en su red interna.
- Notificar a las autoridades de control pertinentes de los incidentes de seguridad, este puede variar según la organización ya que dependerá si cuenta con un Equipo de Respuesta ante Emergencias Informáticas (CERT) o a su vez con un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT).
- Toda información que manipulen los trabajadores en función a su cargo debe ser confidencial caso contrario será sancionado de acuerdo con la LOPDGDD.

Para mejorar los controles de seguridad en una institución se recomienda tomar en cuenta lo siguiente:

- Evitar el uso de equipos informáticos o aplicaciones que no cuenten con garantías con el fin de evitar exponer información confidencial cuando se encuentre trabajando desde casa.
- Contar con software especializados que protejan la información de la organización.
- Mantener actualizado el sistema operativo en conjunto de los programas con los que cuenta la institución.

- Todo servicio o programa que no se esté utilizando o no sea necesario, es recomendable que se encuentre desactivado o en el mejor de los casos desinstalarlo.

- Implementar mecanismos de encriptación o cifrar con alta seguridad todo lo relacionado con la información sensible que comprometan la integridad de los datos que contiene la empresa.

- Configurar reglas de acceso no autorizado para evitar que los empleados naveguen a redes sociales o a sitios web fraudulentos.

Recomendaciones para un SGSI Ecuador

Para la elaboración de un SGSI alineados con la normativa de LOPDP, se deben considerar las siguientes recomendaciones:

- Debe existir un alto compromiso de parte de la gerencia o dirección de la institución u organización interesada en implementar un SGSI, tomando en cuenta que en la LOPDP establece una responsabilidad legal en cuanto al manejo de datos, la nueva entidad de regulación y control garantizará las funciones y atribuciones.

- Estar alineados con las entidades de control y de certificación que garantizarán el correcto manejo de los datos y por ende la organización será la beneficiaria de un buen SGSI, que contará con las políticas más adecuadas a lo que la norma indica para evitar en conjunto que la implementación llegue a fracasar.

- Establecer un ámbito de aplicación según el giro económico de cada institución, esto permitirá definir correctamente el segmento o grupos de riesgos a los cuales están sujetos, para ello la LOPDP define las categorías especiales de datos, las mismas que aclaran cada una las particularidades para regular el tratamiento y derechos tanto de los datos, así como de los beneficiarios de la información.

- Definir correctamente el alcance de la implementación, más aún hoy con la LOPDP que permite establecerlos con propósitos más específicos, siendo por aplicación material y por aplicación territorial, es claro que no tener un alcance viable puede ocasionar que el proceso de levantamiento de información pueda tardar más de lo planificado o en el peor de los casos pueda finalizar prematuramente si se acaparan muchos procesos durante el alcance.

- Definir si el SGSI a desarrollar bastará con seguir todos los controles de seguridad, la LOPDP determina una adecuada seguridad de protección acorde al ámbito, los riesgos, métricas y evaluaciones, el desarrollo de un nuevo SGSI alineado a la LOPDP debe estar sujeto a cambios aplicables en la norma y no regirse obligatoriamente a todos los controles.

- Evaluarse constantemente, es un mecanismo que garantizará el buen funcionamiento de un SGSI y sobre todo permitirá a los interesados de la organización determinar si está completo o debe modificarse. El mal funcionamiento de un SGSI podría incurrir en sanciones económicas o legales según el régimen sancionatorio vigente en la LOPDP.

- Adaptarse al día a día es algo fundamental frente a los cambios tecnológicos y parte vital de un SGSI, si este no se adapta con el tiempo puede llegar a no ser tan fiable. Un SGSI debe ser sostenible a lo largo del tiempo por ello, la responsabilidad proactiva de la organización permitirá que esté actualizado y más aún frente a posibles auditorías y futuras certificaciones.

- Establecer correctamente los roles que participarán durante el proceso de levantamiento, el recurso humano es un factor que no se debe tomar muy a la ligera durante la recopilación de información, ya que al no definir correctamente el rol de un participante podría ocasionar que el proceso no cuente con todo lo necesario para definir el alcance, los riesgos y controles. Con la LOPDP se debe procurar incorporar dos nuevos roles para el tratamiento de los datos, que son el responsable y el encargado, estos dos

roles deberán tomar un papel importante en la toma de decisiones durante la definición de las políticas.

- Comprometer a todo el personal tanto interno como externo de la organización al fiel cumplimiento de las políticas durante el levantamiento y después de puesta en marcha el SGSI, contar con un personal comprometido es reducir la incertidumbre de la resistencia al cambio, ya que están activamente participando con la organización y formarán parte de la visión del negocio como un activo importante.

6. Conclusiones

Con el análisis de ambas Leyes vigentes tanto en Ecuador como en España, se puede concluir lo siguiente:

- Los hechos que causan conmoción con respecto al robo de información fueron los disparadores que permitieron a ambos países replantear sus distintas leyes, con el fin de presentar los mejores controles que garanticen una debida protección de los datos personales de sus ciudadanos, en el caso de España su ley vigente tiene fuertes bases de la ley de protección que rige en el continente europeo, aunque con ciertas particularidades adaptadas a las necesidades y exigencias de dicho país. En cambio, Ecuador toma ciertos lineamientos de la ley europea, pero se centra más en la distinción de los roles y especialmente en el alcance que pueden trabajar según el giro económico.
- Las tipificaciones de los delitos informáticos en ambos países se encuentran correctamente descritos y clasificados según sus Códigos Penales. En España, al tener una ley de protección de datos con mucho más tiempo de experiencia, se puede notar lo estrictas que pueden llegar a ser las infracciones en casos de incumplimiento de la ley, tanto en tiempo de penalización, así como el valor económico causado por multas, los cuales no se ajustan a la realidad económica en Ecuador, a pesar de ello, Ecuador también tiene claramente tipificado los delitos informáticos pero a diferencia de España las penas privativas de la libertad son más exigentes, rondando entre los 4 a 6 años como máximo, por otro lado las sanciones económicas no se acercan a las impuestas en España, aun así en el modelo de multas impuestas en la nueva ley si se considera un porcentaje significativo sobre el volumen del negocio.
- Se puede concluir que la nueva Ley de Protección de Datos en Ecuador, tiene un diseño muy claro en cuando a la especificación de cada artículo, se puede

notar que los mismos fueron redactados con un detalle particular según el actor o rol, ámbito de aplicación, alcance y sobre todo primando los derechos y principios. A la fecha de culminación de este trabajo no está definida la entidad u organismo que se encargará de hacer cumplir y respetar lo que la ley indica, con todo esto la nueva LOPDP presenta un futuro muy prometedor en cuanto a proteger los derechos de los ciudadanos.

- Con la LOPDP vigente en Ecuador es de vital importancia que los SGSI dentro de las organizaciones públicas y privadas, cuenten con todos los ajustes necesarios para estar alineados con las disposiciones de la ley vigente, tomando en cuenta que el capítulo IX “Régimen sancionador” establece las condiciones para efectuar las sanciones correspondientes por el incumplimiento de las normas y sobre todo que determina dos figuras: el encargado y el responsable, quienes deben procurar que la información esté con todos los mecanismos de protección ya que el incumplimiento de alguna normativa recaerá sobre estas dos figuras.
- En conclusión, la implementación de un SGSI es importante debido a que mejora la reputación de la empresa o institución y a la vez cumple con la ley de protección de datos como lo indica tanto para la LOPGDD de España como para la LOPDP de Ecuador.

7. REFERENCIAS

ACEN. (2018). *LA IMPORTANCIA DE CUMPLIR CON LA LEY DE PROTECCION DE DATOS*. Obtenido de https://www.acennavarra.com/la-importancia-de-cumplir-con-la-ley-de-proteccion-de-datos/

Agencia Estatal Boletín Oficial del Estado. (1978). *Constitución Española.* Obtenido de https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

ALBALEGAL ABOGADOS. (10 de Diciembre de 2021). *Historia de la Protección de Datos*. Obtenido de https://www.albalegal.es/historia-de-la-proteccion-de-datos/#:~:text=Nuestro%20primer%20antecedente%20normativo%20nos,de%20Car%C3%A1cter%20Personal(LORTAD)

Alzaga Villamil, Ó. (2000). En torno al concepto de Ley Orgánica en la Constitución. Teoría Y Realidad Constitucional. (1), 115-142. doi:https://doi.org/10.5944/trc.5.2000.6500

Asamblea Nacional del Ecuador. (16 de marzo de 2022). *Defensoría Pública del Ecuador*. Obtenido de https://biblioteca.defensoria.gob.ec/bitstream/37000/3427/1/C%c3%b3digo%20Org%c3%a1nico%20Integral%20Penal.pdf

Bdr Informática y Comunicaciones. (25 de Noviembre de 2020). *¿Conoces los orígenes de la ciberseguridad?* Obtenido de https://bdrinformatica.com/conoces-los-origenes-de-la-ciberseguridad/

Bulnes Aldunate, L. (1984). La ley orgánica Constitucional. *Dialnet, 11*, 227-239.

CARRILLO VINUEZA, D. J., & CORTEZ OVIEDO, D. K. (Julio de 2019). *Universidad Politécnica Salesiana.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/17581/1/UPS%20-%20ST004159.pdf

Castillo, A. (2021). *Creeper, el primer virus informático de la historia, cumple 50 años.* España: 20 minutos.

CISCO. (2022). *¿Qué es la ciberseguridad?* Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Consejo Editorial. (12 de Junio de 2015). *PBP*. (PBP) Recuperado el 9 de Septiembre de 2022, de https://www.pbplaw.com/es/infografia-como-crean-leyes-ecuador

Deloitte. (2020). Estado Actual de la. *IT Ahora*, 8-10.

Division Computer Forensic. (2022). *Legislación*. Obtenido de https://www.delitosinformaticos.info/delitos_informaticos/legislacion

Editorial Etecé. (5 de Agosto de 2021). *Concepto*. Obtenido de https://concepto.de/ley-organica/

Fiscalía General del Estado. (Diciembre de 2021). *Ciberdelito.* Obtenido de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Flores, C. (2018). TIPOS DE HACKERS. *Revista Boliviana*, 16-18.

Galvez, L. (9 de Octubre de 2019). *Ciberseguridad en las redes eléctricas.*

Grupo Atico34 . (8 de Julio de 2022). *Infracciones y Sanciones LOPDGDD/RGPD: criterios, procesos y ejemplos*. Obtenido de https://protecciondatos-lopd.com/empresas/infracciones-sanciones-lopdgdd-rgpd/

Guerrón, J. (16 de Junio de 2021). *ECUADOR Y SU PRIMERA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. Obtenido de https://dpd.aec.es/ecuador-y-su-primera-ley-organica-de-proteccion-de-datos-personales

Gutiérrez, C. (12 de Noviembre de 2013). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2013/11/12/top-10-condenados-por-delitos-informaticos-quienes-fueron-primeros-historia/

Himanen, P. (2001). *The Hacker Ethic.* New York: Random House Trade.

HURTADO PÉREZ, A. J., & ROBAYO GONZÁLEZ, O. (2019). *Repositorio Institucional Universidad Piloto de Colombia.* Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6433/SGSI%20-%20FEBOR%20-%20Trabajo%20de%20Grado.pdf

IBM. (2022). *¿Qué es la ciberseguridad?* Obtenido de https://www.ibm.com/es-es/topics/cybersecurity

Infinito Digital. (16 de Septiembre de 2019). *La filtración de datos en boca de todos.* Obtenido de http://indi.ups.edu.ec/en-boca-de-todos-con-la-filtracion-de-datos-2

J Martelo, R., E Madera, J., & D Betín, A. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Scielo, 26*(2), 129-134. doi:10.4067/S0718-07642015000200015

José Zambrano, K. D. (28 de Abril de 2016). *Delito Informático. Procedimiento Penal en Ecuador*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=5761561

Kaspersky. (2022). *¿Qué es la ciberseguridad?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lejarza, E. (2014). CIBERGUERRA, LOS ESCENARIOS DE CONFRONTACIÓN. *Pre-bie3*(1), 1-20.

Loredo, J. (Junio de 2013). *Delitos Informáticos: su clasificación y una visión general de las medidas de acción de combatirlo*. Obtenido de http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Meléndez, J. (25 de Julio de 2018). *DELITOS INFORMÁTICOS O CIBERDELITOS*. Obtenido de https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/

Morales, D. (2016). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015. *Universidad Señor de Sipan*, 2-135.

Naranjo Martínez & Subía. (30 de Mayo de 2021). *ENTRA EN VIGENCIA LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. Obtenido de https://nmslaw.com.ec/ley-organica-proteccion-datos-personales/#:~:text=Tiene%20por%20objeto%20garantizar%20el,as%C3%AD%20como%20su%20correspondiente%20protecci%C3%B3n.

Observatorio Guatemalteco de Delitos Informáticos - OGDI. (2022). *Historia del Cibercrimen*. Obtenido de https://ogdi.org/historia-del-cibercrimen

Primicias. (16 de Septiembre de 2022). *Así son los costos laborales en Ecuador frente a Latinoamérica*. Obtenido de

https://www.primicias.ec/noticias/economia/latinoamerica-costos-laborales-comparacion/).

Ramirez, R. (27 de diciembre de 2017). *Delitos informáticos establecidos en el COIP y como prevenirlos*. Obtenido de https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Reinares, D. (27 de Septiembre de 2020). *Origen e importancia de la ciberseguridad*. Obtenido de https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/

Revista Seguridad 360. (23 de diciembre de 2021). *Conozca los tipos de delitos informáticos más frecuentes.* Obtenido de https://revistaseguridad360.com/destacados/tipos-de-delitos-informaticos/

Ruiz, J. (2015). Ciberguerra, entorno global y preparación de defensas. Bogota: Universidad Piloto de Colombia.

Ruiz, M. (26 de Agosto de 2021). *El régimen sancionatorio en materia de protección de datos personales*. Obtenido de https://www.avl.com.ec/el-regimen-sancionatorio-en-materia-de-proteccion-de-datos-personales

Salcedo, O., Fernández, C., & Catellanos, L. (2012). HACKERS EN LA SOCIEDAD DE LA INFORMACIÓN: ANÁLISIS DE SU DINÁMICA DESDE UNA PERSPECTIVA SOCIAL. *Visión Electrónica, VI*(1), 115-225.

Saltos, M., Robalino, J., & Pazmiño, L. (2021). ANÁLISIS CONCEPTUAL DEL DELITO INFORMÁTICO EN ECUADOR. *scielo, XVII*(78), 343-351.

Social, D. d. (9 de Noviembre de 2021). *Ley de Protección de Datos Personales*. Obtenido de https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Soto, D., Castillo, F., & Barría, C. (30 de Septiembre de 2021). *Effects of the COVID-19 Pandemic on E-learning Student's Dropout Levels During Cybersecurity Programs: A Case Study.* Obtenido de https://ieeexplore.ieee.org/document/9600381

Stallman, R. (2009). Sobre el hacking. *2002*, 30.

Statista. (29 de Noviembre de 2021). *Número de victimizaciones por ciberdelitos en España de 2011 a 2020*. Obtenido de https://es.statista.com/estadisticas/814010/cibercrimen-numero-de-victimizaciones-espana/

TOALA, Y. (Junio de 2021). *DELITOS INFORMÁTICOS FRECUENTES EN EL ECUADOR: CASOS DE ESTUDIO.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/20942/1/UPS-GT003389.pdf

Universidad de Almeria. (4 de Junio de 2020). *La Ciberseguridad en el Marco Europeo. El caso de España*. Obtenido de http://repositorio.ual.es/handle/10835/9544

Villena, E. (10 de Diciembre de 2021). *Historia de la Protección de Datos*. Obtenido de https://www.albalegal.es/historia-de-la-proteccion-de-datos/

Wikidat. (s.f.). *Delito informático*. Obtenido de https://es.wikidat.com/info/delito-informatico

Yepes, S. (22 de Diciembre de 2021). *Teaching and online learning practices used in different universities during the Covid-19 crisis: Findings and Challenges.* Obtenido de https://ieeexplore.ieee.org/document/9650397