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 MEXICANA DESDE UN ENFOQUE DE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

AUTORES:

LUZ MARÍA IZA NOROÑA
GERARDO ANTONIO MORA CEDEÑO

DIRECTOR:

MIGUEL ARTURO ARCOS ARGUDO

CUENCA – ECUADOR
2023

Autores:

Luz María Iza Noroña
Ingeniera en Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
lizano@est.ups.edu.ec

Gerardo Antonio Mora Cedeño
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
gmora@est.ups.edu.ec

Dirigido por:

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

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

DEDICATORIA

Dedicado a mis padres, María Noroña y Ángel Iza por su amor, por estar conmigo, por enseñarme a crecer y a que si caigo debo levantarme, por apoyarme y guiarme, por ser las bases que me ayudaron a llegar hasta aquí.

A mis hermanos Diego y Sthefany por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias.

A toda mi familia en especial a mi madrina sarita por extender su mano en momentos difíciles, porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Finalmente, dedicado a todas aquellas personas que de una u otra manera sea cual fuera su circunstancia o situación persiguen un objetivo hasta alcanzarlo.

Luz Iza Noroña.

DEDICATORIA

Este logro académico está dedicado con amor y gratitud a mi esposa, a mi hijo, a mis padres y todos aquellos que han estado a mi lado a lo largo de esta travesía.

Cada página de esta tesis lleva impregnada la colaboración, el esfuerzo y el apoyo que he recibido de ustedes.

Que este logro sea un recordatorio de que, con amor, apoyo y determinación, los sueños pueden convertirse en realidad.

Gerardo Mora Cedeño.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por siempre estar a mi lado brindándome ánimo y el apoyo incondicional.

De igual manera mis agradecimientos a la Universidad Politécnica Salesiana, al personal de la Maestría en Seguridad de la Información, quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Finalmente quiero expresar mi más grande y sincero agradecimiento al Ing. Miguel Arcos, Ph.D., principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo.

Luz Iza Noroña.

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a mi amada esposa y a mi querida familia por su inquebrantable apoyo a lo largo de estos años de estudios. Sin su constante respaldo, habría sido imposible alcanzar este logro académico. Sus palabras de aliento y comprensión han sido un pilar fundamental en mi camino hacia la culminación de esta maestría.

Agradezco a mi compañera de tesis, cuya colaboración y compromiso han enriquecido este proceso de investigación. Juntos hemos superado desafíos y hemos trabajado arduamente para alcanzar nuestros objetivos académicos.

Además, quiero extender mi gratitud a mi dedicado tutor PhD. Miguel Arcos Argudo, cuya orientación y conocimientos han sido fundamentales en el desarrollo de esta tesis

Gerardo Mora Cedeño

Tabla de Contenido

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

Autores:
Luz María Iza Noroña
Gerardo Antonio Mora Cedeño

Resumen

El presente trabajo se enfoca en identificar similitudes, diferencias y desafíos comunes en las leyes de protección de datos en Ecuador y México, y proporcionar un análisis de cómo estas regulaciones influyen en la privacidad de los ciudadanos y el manejo de datos personales.

El análisis se realiza a través de un enfoque interdisciplinario que abarca aspectos legales y tecnológicos, considerando la evolución de estas leyes a lo largo del tiempo y su alineación con los estándares internacionales de protección de datos.

Además del análisis comparativo, esta tesis también ofrece valiosas recomendaciones para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Estas recomendaciones están diseñadas para ayudar a las organizaciones en Ecuador y México a garantizar el cumplimiento de las leyes de protección de datos y fortalecer sus medidas de seguridad de la información.

El SGSI se presenta como una herramienta clave para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, alineando las actividades de las organizaciones con las regulaciones de privacidad vigentes.

Palabras clave:

Ley Orgánica de Protección de Datos Personales, Sistema de Gestión de Seguridad de la Información, Datos Personales, Consentimiento, Tratamiento de Datos Personales, Delitos Informáticos, Derechos.

Abstract

This work is focused on identifying similarities, differences, and common challenges in data protection laws in Ecuador and Mexico and providing an analysis of how these regulations influence citizens privacy and the handling of personal data.

The analysis is carried out through an interdisciplinary approach covering legal and technological aspects, considering the evolution of these laws over time, and their alignment with international data protection standards.

In addition to the comparative analysis, this thesis also provides valuable recommendations for implementing an Information Security Management System (ISMS). These recommendations are designed to assist organizations in Ecuador and Mexico in ensuring compliance with data protection laws and strengthening their information security measures.

The ISMS is presented as a key tool for ensuring the confidentiality, integrity, and availability of personal data, aligning organizations activities with current privacy regulations.

Keywords:

Organic Law on Data Protection, Information Security Management System, Personal Data, Consent, Personal Data Processing, Cybercrimes, Rights.

1 INTRODUCCIÓN

En el mundo digital actual, la protección de datos personales y la seguridad de la información se ha convertido en un tema cada vez más relevante. La creciente interconexión y el aumento del uso de Tecnologías de la Información y Comunicación (TICs) han dado lugar a un aumento en los riesgos de ciberseguridad y delitos informáticos. Ante este escenario, los países han desarrollado marcos legales para definir los derechos de los individuos, protegerlos y regular el tratamiento de los datos personales. En América Latina, Ecuador y México son dos países que han implementado medidas para proteger los datos personales.

En este contexto, la presente tesis tiene como objetivo realizar un análisis comparativo de las leyes de protección de datos personales en Ecuador y México, centrándose en el enfoque de ciberseguridad y delitos informáticos; examinar las similitudes y diferencias de sus marcos legales, identificar las mejores prácticas y los desafíos en la protección de datos en el entorno digital. De esta manera, se pretende comprender mejor las regulaciones de protección de datos en estos países y su relevancia en la protección de los derechos fundamentales de las personas.

2 Determinación del Problema

La protección de datos personales y la preservación de la privacidad se han convertido en grandes desafíos. La recopilación, el almacenamiento y el procesamiento de datos personales son prácticas habituales en las operaciones de empresas, organizaciones y gobiernos en todo el mundo. En este contexto, Ecuador y México han promulgado leyes de protección de datos personales destinadas a salvaguardar la privacidad y la seguridad de la información personal de sus ciudadanos.

En septiembre de 2019, se dio a conocer a nivel internacional que una brecha de seguridad en un servidor había expuesto los datos personales de aproximadamente 20 millones de ecuatorianos, considerada hasta ese momento como la filtración de datos más grande en Ecuador. Como resultado, el 19 de septiembre de 2019, durante el mandato del presidente Lenin Moreno, se presentó ante la Asamblea Nacional el proyecto de la Ley Orgánica de Protección de Datos Personales.

En 2021, la Comisión Económica para América Latina y el Caribe (CEPAL) informó que el 66,7% de la población latinoamericana tenía acceso a internet en sus hogares [1], lo cual representa un crecimiento de la penetración de usuarios de internet, y por consiguiente un aumento de las amenazas. En respuesta a esto, la legislación penal ha establecido artículos que abordan diversos tipos de ataques, como la pornografía digital, estafas y actividades ilícitas, entre otros, que se detallan en el Código Integral Penal de Ecuador [2].

El 26 de mayo de 2021, se publicó en el Registro Oficial de la Ley Orgánica de Protección de Datos Personales, un período de adaptación de 2 años para que las empresas ajusten sus procesos a las disposiciones de la norma. Esta ley garantiza a los titulares de datos nueve derechos, “acceso, rectificación y actualización, eliminación, oposición, portabilidad, limitación de tratamiento, a no ser objeto de

una decisión basada únicamente en valoraciones automatizadas, consulta, educación digital" [3].

En el caso de México, existen dos leyes principales relacionadas con la protección de datos personales:

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), regula el tratamiento de datos por parte de empresas del sector privado desde el 5 de julio de 2010 [4].
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), establece normas para el tratamiento de datos por parte de entidades del sector público desde el 26 de enero de 2017 [5].

Ecuador y México realizan esfuerzos por establecer marcos legales sólidos, sin embargo existen desafíos como: crear conciencia sobre la importancia del cumplimiento de las Leyes de Protección de Datos Personales en todos los niveles de la organización, garantizar que se obtenga un consentimiento adecuado para recopilar y procesar datos personales, asegurar que los datos estén protegidos contra violaciones de seguridad, mantener registro detallado del tratamiento que se da a los datos personales, notificación oportuna de las violaciones de datos a las autoridades de control y los titulares.

Existe la necesidad de evaluar de manera comparativa las leyes de protección de datos en Ecuador y México, identificar similitudes, diferencias y efectividad de estas leyes. Además, este análisis comparativo permitirá identificar áreas donde estas regulaciones pueden ser mejoradas o fortalecidas.

3 Estado del arte

3.1 Reseña Histórica

3.1.1 Primeros delitos informáticos

Los primeros delitos informáticos pueden rastrearse en la década de 1960. Durante ese tiempo, algunos programadores informáticos buscaron sabotear el financiamiento de la guerra de Vietnam por parte del gobierno estadounidense y encontraron una forma de proporcionar servicios telefónicos gratuitos a la población. Estos individuos, conocidos como phreakers o piratas telefónicos, utilizaban equipos para enrutamiento de llamadas telefónicas de larga distancia, simulando los tonos de llamadas de compañías prominentes como AT&T y Bell Corporation [6].

En la década de 1970 los delitos informáticos se caracterizan principalmente por el sabotaje, la piratería y el espionaje. En relación con el sabotaje, esta era la principal preocupación de las empresas proveedoras de servicios e instituciones de gobierno debido al gran volumen de datos almacenados y a la criticidad de la pérdida de disponibilidad. Estos ataques incluían daños tanto a los dispositivos de almacenamiento como a las instalaciones, así también a la infraestructura de red.

Con respecto a la piratería, esta se caracterizaba por la copia de software de computación sin autorización para luego ser comercializado. Y en lo relacionado al espionaje, la extracción de información se realizaba directamente desde los dispositivos de almacenamiento haciendo uso de técnicas de ingeniería social para la obtención de códigos y contraseñas. Entre los principales objetivos de información se encontraban los datos contables de empresas, datos de clientes corporativos potenciales, datos de investigaciones, entre otros [6].

En la década de 1980 existe un notable incremento de los delitos informáticos y se convirtieron en una amenaza más seria, cuando los hackers comenzaron a buscar activamente vulnerabilidades en los sistemas informáticos y a desarrollar software malicioso para explotarlas. Estos delitos se caracterizan por los fraudes informáticos mediante la adulteración de tarjetas de crédito, la distribución de contenido ilícito, pornografía infantil, incitación al odio y racismo. También aparecen ataques que adulteran información de afiliados a servicios de salud y seguridad social. Durante esta década los países de Europa tienen la iniciativa de generar y promover leyes y normas para proteger dinero electrónico, datos personales y otros bienes inmateriales [6].

3.1.2 Autores de los primeros delitos informáticos

Son varios los delitos que se han realizado a lo largo de los años, a continuación, se presenta una lista cronológica de los autores de los primeros delitos informáticos desde la década de 1960 hasta la década de 1990:

En 1962, Allan Scherr, estudiante de la MIT, diseña una tarjeta perforada para que el computador de la Universidad imprima los usuarios y contraseñas de otros estudiantes para obtener más tiempo en el acceso a los computadores. Es considerado el primer “Troll” [7].

En 1981, Ian Murphy, quien también era conocido con el seudónimo de “Capitan Zap”, hackeó las computadoras de AT&T y cambiaba el reloj interno de facturación de tal forma que los clientes obtuvieran descuentos durante las horas pico. Es considerada la primera persona en ser condenado por un delito cibernético [8].

En 1988, Robert Morris lanzó en ARPANET (Advanced Research Projects Administration Network) el primer gusano apodado “The Morris Worm”. Su intención era mapear el Internet, pero un error en su código, hizo que este se propague y duplique sin control, infectando miles de computadoras y causando

interrupciones considerables en la red. Este ataque fue lanzado desde un computador de la Universidad de Massachussets [8].

En 1988, Kevin Mitnick realizó un ataque notable al sistema informático de DEC (Digital Equipment Corporation) y de MCI Comunication, empresas de tecnología y seguridad de aquel entonces. Este ataque le permitió acceder a información confidencial y fue uno de los casos que lo puso en el radar de las autoridades [9]. Sin embargo, fue en la década de 1990 cuando Kevin Mitnick se convirtió en uno de los hackers más buscados por el FBI. Sus actividades delictivas, que incluían la intrusión en sistemas de grandes corporaciones y agencias gubernamentales, lo llevaron a ser arrestado en 1995 [9].

3.1.3 Sanciones a los primeros delitos informáticos

En la década de 1960 y 1970, cuando se cometieron los primeros delitos informáticos, no existían leyes específicas para castigar este tipo de acciones. Por lo tanto, en algunos casos, los autores no fueron sancionados. En otros casos, las sanciones impuestas fueron mínimas, ya que los daños causados eran considerados menores o no se conocían las implicaciones de los delitos informáticos en aquel momento.

En 1990, Robert Morris fue juzgado bajo la "Ley de Fraude y Abuso Informático" de los Estados Unidos de Norteamérica y condenado a 3 años de libertad condicional, 400 horas de servicios comunitarios y al pago de una multa de 10 mil dólares, por encontrarlo culpable del cargo de: "Acceso intencional a computadoras de interés federal sin autorización…" [8]. Este incidente llevó a una mayor conciencia sobre la importancia de la seguridad informática y la necesidad de proteger las redes. Robert Morris pasó a convertirse en un respetado investigador en seguridad informática y cofundó la empresa de inversión en tecnología "Y Combinator".

En 1995, Kevin Mitnick fue arrestado debido a una serie de actividades ilegales relacionadas con la piratería informática. Su arresto marcó el final de una extensa

búsqueda por parte del FBI, y requirió la colaboración de compañías de seguridad informática. Fue condenado a 5 años de prisión [9].

3.1.4 Primeros países que aprobaron una ley de protección de datos personales (LPDP)

La creación de leyes de protección de datos personales en el mundo es reciente y refleja la evolución de la sociedad. La Asamblea Consultiva del Consejo de Europa creada en 1967, desempeñó un papel fundamental en este proceso, donde se analizó la necesidad de proteger la privacidad de los individuos debido a los avances tecnológicos y cambios socioculturales [10].

EN EUROPA

Suecia - La Ley de Protección de Datos Personales de 1973

Suecia fue pionera en la promulgación de una ley de protección de datos personales en 1973. Esta ley estableció los principios fundamentales para el procesamiento de datos personales, garantizó los derechos individuales y estableció límites al uso de la informática. La ley sueca sentó las bases para futuras legislaciones de protección de datos en toda Europa [11].

Alemania - La Ley Federal de Protección de Datos de 1977

En Alemania, la Ley Federal de Protección de Datos de 1977 fue una de las primeras leyes integrales de protección de datos en Europa. Esta ley tiene como principio impedir la transmisión de datos sin autorización del individuo. También creó la Oficina del Comisionado Federal de Protección de Datos, encargada de supervisar la aplicación de la ley y proteger la privacidad de los ciudadanos [12].

Francia - La Ley Informática, los Ficheros y las Libertades de 1978

En Francia, la “Ley Informática, los Ficheros y las Libertades” de 1978 fue un hito importante en la protección de datos personales. Esta ley otorga derechos a las personas para impugnar las decisiones tomadas con relación al uso de los datos.

Además, la ley estableció la Comisión Nacional de Informática y Libertades (CNIL), una autoridad independiente y con presupuesto propio, encargada de velar el cumplimiento de la ley, denunciar infracciones ante el Ministerio y la toma de medidas que fuesen necesarias para realizar sus funciones [13].

España - La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 1992

En España, la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 1992, también conocida como LORTAD, fue una de las primeras normas en abordar la protección de datos personales en el país. Esta ley estableció principios relacionados al tratamiento de los datos personales, derechos al acceso, rectificación, cancelación e impugnación. Esta ley también limita el uso de la informática [11].

EN LATINOAMERICA

Chile - La Ley sobre Protección de la Vida Privada de 1999

En Chile, la Ley sobre Protección de la Vida Privada fue promulgada en el año 1999 y se convirtió en la primera ley de este tipo en América Latina. Esta ley establece normativas significativas en lo que concierne al manejo de datos personales en registros, tanto por parte de entidades públicas como privadas, siendo uno de los marcos legales más importantes en este ámbito. Esta ley reconoce el derecho de las personas al acceso, rectificación y cancelación [14].

Argentina - La Ley de Protección de Datos Personales de 2000

En Argentina, la Ley de Protección de Datos Personales N° 25.326 fue promulgada en el año 2000 y fue inspirada en la ley española del año 1992. Esta ley busca proteger los datos personales en archivos, bases de datos u otros medios y estableció el consentimiento informado por parte de los titulares para el tratamiento de datos personales, siempre que los mismos no sean obtenidos de

fuentes de acceso público. Además, establece la obligatoriedad de informar a los titulares la finalidad del tratamiento de los datos personales [15].

Uruguay - La Ley de Protección de Datos Personales y Acción de Habeas Data de 2008

En Uruguay, la Ley de Protección de Datos Personales N° 18.331 fue aprobada en el año 2008. Esta normativa abarca los datos personales registrados en cualquier medio que posibilite su procesamiento y uso en diferentes contextos, ya sea en el ámbito privado o público. También se creó la Unidad Reguladora y de Control de Datos Personales (URCDP), encargada del cumplimiento de la ley y proteger la privacidad de los ciudadanos [16].

3.2 Definiciones principales

En esta sección se establecerán los principales conceptos y definiciones para la adecuada comprensión de este trabajo.

3.2.1 Hacker

Para referirnos a los piratas informáticos o hackers podemos citar a autores como Erickson quién lo define como la persona que resuelve problemas de forma inimaginables en comparación a aquellos que se limitan a resolverlos con métodos convencionales. Mientras que Sweigart lo define como un individuo que estudia un sistema para comprenderlo y ser capaz de modificarlo de varias formas, la mayoría de ellas creativas [17]. Se coincide que, en efecto, un hacker posee conocimientos profundos y evidenciables de sistemas, ya sean estos en el área de sistemas informáticos, arquitectura, infraestructura, comunicaciones u otros campos. No obstante, es la falta de autorización de los propietarios de los sistemas lo que incurren en actos de ilegalidad que muchas veces terminan en actos delictivos [17].

3.2.2 Hacker ético

Se define al hacker ético como la persona que tiene experticia en el uso de computadores, networking, programas informáticos, etc., cuya actividad principal es el realizar ataques controlados a los sistemas de seguridad previa autorización de los propietarios, con el objetivo de identificar vulnerabilidades y brechas de seguridad que un hacker malicioso podría aprovechar [17].

3.2.3 ¿Qué es un SGSI?

Un Sistema de Gestión de Seguridad de la Información (SGSI), es considerado un conjunto de tecnologías, procedimientos y políticas de administración diseñados para para proteger y garantizar la seguridad y confidencialidad de la información. Esta implementación puede estar guiada principalmente por la norma ISO/IEC:27001, el cual es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la International Electrotechnical Commission [18].

Un SGSI se basa en la evaluación y la mejora continua y en este contexto, el Ciclo de Deming, también conocido como el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), proporciona un enfoque de gestión que se utiliza para mejorar procesos y sistemas, y se puede aplicar al desarrollo, implementación y mantenimiento de un SGSI de la siguiente manera:

- Plan (Planificar): en esta fase se establecen los objetivos y metas del SGSI. Se identifican los riesgos de seguridad de la información, se definen políticas y se determinan los controles de seguridad adecuados.
- Do (Hacer): en esta fase se implementan las políticas definidas en la planificación y se aplican los controles de seguridad.
- Check (Verificar): en esta fase se evalúa el desempeño (eficiencia y eficacia) del SGSI. Se realizan auditorías internas y evaluaciones de cumplimiento.
- Act (Actuar): en esta fase se toman medidas correctivas y preventivas en función de los resultados de la fase de verificación.

La retroalimentación constante, la adaptación y la mejora son elementos esenciales en la gestión exitosa de la seguridad de la información.

3.2.4 ¿Qué es una Ley Orgánica?

Una ley orgánica es una categoría especial de legislación que se caracteriza por su importancia y jerarquía en el sistema legal de un país, ya que se relaciona directamente con la organización y funcionamiento de las instituciones gubernamentales y otros aspectos fundamentales de la vida política y jurídica. Estas leyes suelen regular asuntos de gran relevancia, como los derechos fundamentales, la estructura del Estado, las competencias de los poderes públicos y otros aspectos esenciales de la vida institucional. De acuerdo a Kelsen, “las Leyes Orgánicas son inferiores en rango a la Constitución, pero superiores a las ordinarias” [19].

En Ecuador y México la definición legal de datos personales es similar. La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador define los datos personales como "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas naturales o jurídicas identificadas o identificables" [3]. En México, la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) define los datos personales como "cualquier información concerniente a una persona física identificada o identificable" [4].

3.2.5 ¿Qué son datos personales?

Los datos personales se definen como cualquier información relacionada a una persona que puede ser recopilada y permite la identificación; tales como: documento de identidad, nombres, apellidos, dirección domiciliaria, correo electrónico, números telefónicos de localización, entre otros. Así mismo se debe mencionar que existen datos que pueden ser catalogados sensibles, entre los que

se encuentran historiales médicos, orientación sexual, creencias religiosas, entre etc., los mismos que pueden afectar la intimidad familiar y personal [20].

3.3 Delitos informáticos en Ecuador

En Ecuador, los delitos informáticos se encuentran definidos y sancionados en el Código Orgánico Integral Penal (COIP) como parte de un mecanismo de persecución y establecimiento de penas. De acuerdo a información de la Fiscalía General del Estado, en los últimos tres años, los delitos informáticos más frecuentes denunciados entre los años 2019 y 2021 se presentan en la Tabla 1:

ART. COIP	TIPO PENAL /ARTICULO	Frecuencia por año			
		2019	2020	2021	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	81	113	95	**289**
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	17	18	15	**50**
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	165	152	152	**469**
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	16	7	7	**30**
178	Violación a la intimidad	2038	1985	1346	**5369**
186	Estafa	16918	18415	16272	**51605**
188	Aprovechamiento ilícito de servicios públicos	194	99	72	**365**
190	Apropiación fraudulenta por medios electrónicos	1744	2280	3962	**7986**
192	Intercambio, comercialización o compra de información de equipos terminales móviles	-	1	1	**2**
193	Reemplazo de identificación de terminales móviles	-	3	-	**3**
194	Comercialización ilícita de terminales móviles	7	285	10	**302**
195	Infraestructura ilícita	7	-	-	**7**
211	Supresión, alteración o suposición de la identidad y estado civil	54	23	28	**105**
229	Revelación ilegal de base de datos	34	30	23	**87**
230	Interceptación ilegal de datos	86	73	35	**194**
231	Transferencia electrónica de activo patrimonial	50	76	170	**296**
232	Ataque a la integridad de sistemas informáticos	111	95	86	**292**
233	Delitos contra la información pública reservada legalmente.	5	5	4	**14**
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	242	295	274	**811**
366	Terrorismo	65	13	17	**95**
	Total General por años	**21834**	**23968**	**22569**	**68371**

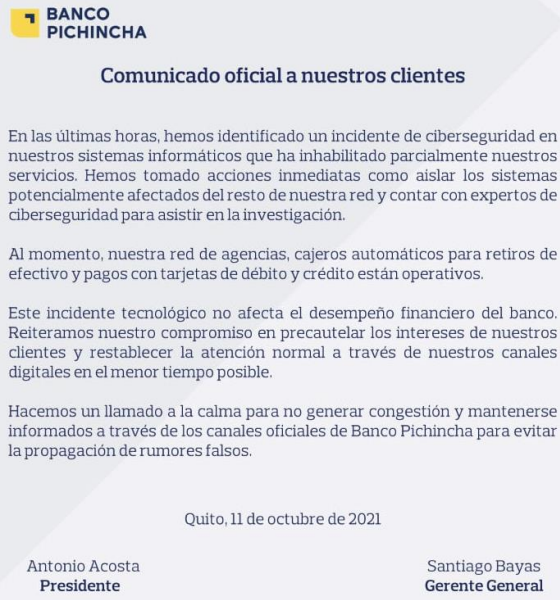
Tabla 1. Estadística Delitos Informáticos desde el mes de enero 2019 al mes de agosto de 2021 [21] .

3.3.1 Caso de ciberataque en Ecuador

En el año 2021 se reportó un caso de delito informático a uno de los bancos más grandes de Ecuador (Banco Pichincha). Después de más de 72 horas sin servicio en sus canales electrónicos, dicho banco informó en un comunicado que la falla se debe a un "incidente de ciberseguridad" detectado en sus sistemas informáticos [22].

Miles de usuarios reportaron incidentes y la caída de servicios tanto en la web como en dispositivos móviles, cajeros automáticos y servicios en ventanilla con irregularidades. El delito no solo provocó largas filas en sus sucursales, sino miles de quejas tanto en redes sociales como en algunas ventanillas [22].

Si bien el banco no dio mayores detalles sobre la naturaleza del ataque y comunicó que están trabajando con especialistas e investigando lo que ocurrió, fuentes del portal Bleeping Computer [22] dijeron que se trata de un ataque de ransomware que utiliza la herramienta de pentesting Cobal Strike, la cual suele ser utilizada por los cibercriminales, entre ellos bandas de ransomware [23].



BANCO PICHINCHA

Comunicado oficial a nuestros clientes

En las últimas horas, hemos identificado un incidente de ciberseguridad en nuestros sistemas informáticos que ha inhabilitado parcialmente nuestros servicios. Hemos tomado acciones inmediatas como aislar los sistemas potencialmente afectados del resto de nuestra red y contar con expertos de ciberseguridad para asistir en la investigación.

Al momento, nuestra red de agencias, cajeros automáticos para retiros de efectivo y pagos con tarjetas de débito y crédito están operativos.

Este incidente tecnológico no afecta el desempeño financiero del banco. Reiteramos nuestro compromiso en precautelar los intereses de nuestros clientes y restablecer la atención normal a través de nuestros canales digitales en el menor tiempo posible.

Hacemos un llamado a la calma para no generar congestión y mantenerse informados a través de los canales oficiales de Banco Pichincha para evitar la propagación de rumores falsos.

Quito, 11 de octubre de 2021

Antonio Acosta
Presidente

Santiago Bayas
Gerente General

Figura 1. Comunicado Banco Pichincha, Ecuador [22].

3.3.2 Ataque Informático y Apagón de CNT

El 14 de julio del año 2021, la Corporación Nacional de Telecomunicaciones (CNT) había sido víctima de un ciberataque, es decir, un ataque externo a los sistemas de la empresa [6]. En un inicio, según algunos expertos, se trató de un ataque planificado y sumamente agresivo, aseguraron que la información no fue secuestrada gracias al rápido accionar de apagar los servidores, también se dijo que los sistemas fueron restablecidos, descartando un "contagio" que se extienda o haya extendido a otras entidades estatales [24]. Al cabo de unos días se anunció que la empresa pública de telecomunicaciones sería declarada en emergencia. Se sabe que este ataque fue externo y fue provocado por ransomware EXX, el virus atacó al sistema informático, alterando las áreas de facturación, activaciones y recargas. Según la versión oficial, la noche del 14 de julio de 2021, se habría iniciado el ciberataque contra los sistemas de CNT. El ransomware EXX puede vulnerar diversas instancias como el sitio, la red, las bases de datos y sistemas informáticos [6].

Algunos expertos, dicen que lo sucedido podría ser una combinación de ataques no solo el ransomware, sino también phishing e ingeniería social. En redes sociales se puede ver información que habría sido filtrada, se dice que son cerca de 11 gigabytes los comprometidos de los casi 200 que tiene CNT [24].

4 Metodología

Para el desarrollo de este trabajo se realizó una revisión bibliográfica de las leyes, reglamentos y otros documentos relacionados con la protección de los datos personales en ambos países. Se consultaron fuentes primarias y secundarias, tanto en línea como físicas.

Se llevó a cabo un análisis comparativo entre la Ley Orgánica de Protección de Datos Personales de Ecuador y la Legislación Mexicana en materia de protección de datos personales y delitos informáticos, con un enfoque en la ciberseguridad. Para ello, se utilizará un enfoque descriptivo y comparativo, revisando las similitudes y diferencias entre ambas leyes, así como su eficacia en la protección de los datos personales.

La metodología utilizará principalmente la revisión bibliográfica de documentación relacionada a la temática, lectura comparativa de la legislación de ambos países, redacción sistemática de las conclusiones y recomendaciones que podrían considerarse en un SGSI de acuerdo con el análisis de la normativa de cada país.

4.1 Reseña histórica de la Ley Orgánica de Protección de Datos Personales en ambos países.

La protección de datos personales posee una dimensión global y se encuentra presente en varias leyes y normas de varios países alrededor del mundo. Entre los principales instrumentos normativos se pueden mencionar: Convenio de Europa, ONU, OCDE, Unión Europea, Conferencia de Autoridades de Privacidad, Red Iberoamericana de Protección de Datos Personales [10].

Tanto Ecuador como México han establecido leyes que regulan la protección de datos personales, reconociendo el derecho fundamental de las personas a la privacidad de su información. En este capítulo, se realizará una reseña histórica de la Ley de Protección de Datos Personales en Ecuador y México, examinando su evolución a lo largo del tiempo y su impacto en la sociedad.

En Ecuador, en los últimos años, se ha elaborado un plan de estrategias plasmadas en códigos penales los cuales buscan mitigar y prevenir ataques cibernéticos. La implementación de una política y estrategia en el 2017 incluye a varios documentos para garantizar la seguridad de la información, por ejemplo: Constitución de la República, Ley de Comercio Electrónico, Leyes Orgánicas, entre otros.

4.1.1 En Ecuador

A continuación, presentaremos algunas leyes relacionadas con la protección de datos y privacidad en Ecuador antes de 2021:

La Ley Orgánica De Transparencia Y Acceso a la Información de 2004

Esta ley en su artículo 6 establece que la información personal es confidencial y sanciona su empleo de modo ilegal [25, p. 3].

La ley de Derechos y Amparo del Paciente de 2006

Esta ley en su artículo 4 establece el derecho a la confidencialidad de la información en materia de salud y tratamientos médicos a aplicársele [26]. Esto es reforzado en el artículo 6 de la Ley Orgánica de salud la cual señala que es responsabilidad del Ministerio de Salud Pública garantizar la confidencialidad de la información relacionados a la salud [27].

La Constitución de la República del Ecuador de 2008

En el capítulo sexto “Derechos de Libertad” articulo 66, numeral 19 establece el derecho a la protección de datos de carácter personal, así como la autorización del titular o el mandato de la ley para tratamiento de estos datos. En este sentido, la

Constitución en el artículo 66, numeral 11 garantiza el derecho a la intimidad personal, y en numeral 20 garantiza el derecho a la intimidad, a la inviolabilidad y secreto de correspondencia [28].

Así mismo la Constitución, en el artículo 92, mediante el habeas data, garantiza a las personas el conocimiento y acceso a los documentos, bases de datos personales, informes de sí mismos y de sus bienes que se encuentren en posesión de entidades públicas o privadas [28].

Ley Orgánica de Comunicación de 2013

En sus artículos 30 y 31 restringe la circulación de información relacionado a datos personales sin autorización del titular o de un juez competente a través de los medios de comunicación y protege el secreto de las comunicaciones personales [29, pp. 7, 8].

Código Orgánico Integral Penal de 2014

El COIP contempla leyes que sancionan delitos informáticos con penas privativas de libertad. Esta norma busca garantizar los derechos de las personas, combatir la impunidad y ejecutar penas [30].

Ley Orgánica de Telecomunicaciones de 2015

Incluye un título específico sobre el Secreto de las Comunicaciones y Protección de Datos Personales, la cual indica que los prestadores de servicio de telecomunicaciones deben garantizar en el ejercicio de su actividad la protección de los datos de carácter personal en línea con lo dispuesto por la Constitución [31, p. 22].

Ley Orgánica de Protección de Datos Personales de 2021

Esta ley fue publicada en el Registro Oficial el 26 de mayo de 2021 y busca salvaguardar la privacidad y los derechos de las personas en relación con el tratamiento de sus datos personales.

Esta ley regula a todas las entidades públicas o privadas que realicen el tratamiento de datos personales en Ecuador y define términos como: datos personales, datos personales sensibles, categorías especiales, entre otros. También establece principios para el tratamiento de datos, tales como legalidad, consentimiento, finalidad y proporcionalidad.

Reconoce los derechos ARCO para los titulares de datos, permitiendo control sobre su información personal. Cuando sea creada, la Superintendencia de Protección de Datos, será la entidad encargada de supervisar y hacer cumplir la LOPDP [3].

4.1.2 En México

La evolución de leyes relacionados a la protección de datos y privacidad en México antes de la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010 fue un proceso caracterizado por la falta de normas y definiciones específicas. A continuación, presentaremos una descripción cronológica de las leyes y regulaciones clave relacionadas con la privacidad y la protección de datos en México antes de 2010:

Constitución Política de los Estados Unidos Mexicanos de 1917

La Constitución de México contiene disposiciones que garantizan el derecho a la privacidad y la inviolabilidad de la correspondencia. En el artículo 16 de la Constitución se establece que “Las comunicaciones privadas son inviolables…” [32, p. 18]. Así también, en el año 2009 se adiciona el párrafo: "Toda persona tiene derecho a la protección de sus datos personales… " [32, p. 17].

Ley Federal de Telecomunicaciones y Radiodifusión de 1995

Esta ley regulaba el sector de las telecomunicaciones y la radiodifusión en México y establecía infracciones sobre la interceptación de información transmitida por las reses públicas de telecomunicaciones [33].

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002

Aunque no se centraba exclusivamente en la protección de datos personales, esta ley abordaba la transparencia y el acceso a la información gubernamental. Establecía ciertas restricciones y regulaciones sobre la divulgación de información que podría afectar la privacidad de las personas [34].

Ley Federal de Protección de Datos Personales en Posesión de Particulares en México en 2010

Esta ley fue promulgada el 11 de junio del 2010, establece principios clave que norman el tratamiento de información personal por parte de entidades privadas, priorizando la protección de los derechos de los titulares de datos. Entre los aspectos más destacados se encuentra el requisito de obtener el consentimiento expreso de los titulares antes de recopilar o utilizar sus datos personales, así como la obligación de informar de manera transparente sobre la finalidad del tratamiento. Además, la legislación establece medidas de seguridad que deben ser implementadas para resguardar la confidencialidad y la integridad de los datos, y crea del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como autoridad encargada de supervisar y hacer cumplir la ley, garantizando así su aplicación efectiva [4].

Esta ley promueve una mayor conciencia sobre la importancia de la privacidad en un entorno digital en constante evolución. Su implementación fortalece la confianza de los ciudadanos en la gestión de sus datos personales por parte de las empresas y establece una base legal sólida para salvaguardar la información personal en México.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en 2017

Esta ley fue promulgada el 26 de enero de 2017, establece los fundamentos, principios y procesos necesarios para asegurar el derecho inherente de cualquier individuo a la salvaguardia de su información personal.

Entre los aspectos más destacados se encuentran definiciones más completas sobre datos personales, datos personales sensibles, consentimiento informado, el mismo que debe ser obtenido antes el tratamiento de datos personales. La LGPDPPSO exige la creación y difusión de un Aviso de Privacidad que informe a los titulares sobre el tratamiento de sus datos [5].

4.2 Delitos Tipificados en las Leyes Orgánicas de Protección de Datos Personales en ambos países.

En esta sección, se llevará a cabo un análisis de las disposiciones legales relacionadas con la protección de datos en ambos países. Además, se pretende comprender y comparar las medidas adoptadas en cada país para sancionar las infracciones relacionadas con la privacidad y la seguridad de los datos personales.

4.2.1 Publicación de Ley de Protección de Datos

La fecha de publicación de una Ley de Protección de Datos nos ayuda a comprender las circunstancias específicas que llevaron a su creación, principalmente por la evolución tecnológica, cambios sociales e influencia de estándares internacionales. Esto permite un análisis más preciso y contextualizado al comparar leyes entre diferentes países.

Como se puede observar en la Tabla 2, el primero en publicar una ley de este tipo fue México con la Ley Federal de Protección de Datos Personales en Posesión de Particulares para el sector privado del año 2010 [4]. Siete años más tarde, en 2017 publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos

Obligado para el sector público [5]. En el año 2021, Ecuador publica su primera Ley Orgánica de Protección de Datos Personales para sector público y privado [3].

	Ecuador	México	
Nombre de la Ley	**Ley Orgánica de Protección de Datos Personales**	**Ley Federal de Protección de Datos Personales en Posesión de Particulares**	**Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**
Siglas	LOPDP	LFPDPPP	LGPDPPSO
Fecha de publicación	2021, 26 de mayo	2010, 05 de julio	2017, 26 de enero
A quién regula	Empresas del sector privado y público.	Empresas del sector privado.	Empresas del sector público

Tabla 2. Comparativo de fecha de publicación de Ley de Datos Personales Ecuador y México [3], [4], [5].

Aunque hace algunos años el COIP identificaba y sancionaba ciertos delitos informáticos, es evidente que Ecuador ha llegado tarde en la implementación de una Ley de Protección de Datos Personales. Este asunto es relativamente nuevo y demanda un esfuerzo significativo por parte del Estado para asegurar la protección sólida y clara de los derechos del ciudadano en lo que respecta a sus datos personales.

La Tabla 3 presenta un resumen de la estructura adoptada para redactar la ley en ambos países:

	Ecuador	México	
Tema	**LOPDP**	**LFPDPPP**	**LGPDPPSO**
Aplicación	CAPITULO I. “Ámbito de Aplicación Integral”	CAPÍTULO I. “Disposiciones Generales”	TÍTULO PRIMERO “Disposiciones Generales”
Principios	CAPÍTULO II. “Principios”	CAPÍTULO II. “Los Principios de Protección de Datos Personales”	TÍTULO SEGUNDO “Principios Y Deberes”
Derechos	CAPÍTULO III. “Derechos”	CAPÍTULO III. “Los Derechos de los Titulares de Datos Personales”	TÍTULO TERCERO “Derechos De Los Titulares Y Su Ejercicio”

Responsables y Encargados	CAPITULO VII "Del Responsable, Encargo Y Delegado De Protección De Datos Personales"	CAPÍTULO II. "Los Principios de Protección de Datos Personales"	TÍTULO CUARTO "Relación Del Responsable Y Encargado"
Transferencia	CAPITULO IX. "Transferencia o Comunicación Internacional de Datos Personales"	CAPÍTULO V. "De la Transferencia de Datos"	TÍTULO QUINTO "Comunicaciones De Datos Personales"
Procedimientos	CAPÍTULO X. "De Los Requerimientos Directos Y De La Gestión Del Procedimiento Administrativo"	CAPÍTULO VII. "Del Procedimiento de Protección de Derechos"	TÍTULO DÉCIMO "Facultad De Verificación Del Instituto Y Los Organismos Garantes"
Infracciones y sanciones	CAPITULO XI. "Medidas Correctivas, Infracciones Y Régimen Sancionatorio"	CAPÍTULO X. "De las Infracciones y Sanciones"	TÍTULO DÉCIMO "Primero Medidas De Apremio Y Responsabilidades"
Autoridades de Control	CAPÍTULO XII. "Autoridad de Protección de Datos Personales"	CAPÍTULO VI. "Las Autoridades Sección I. Del Instituto Sección II. De las Autoridades Reguladoras"	TÍTULO OCTAVO "Organismos Garantes"

Tabla 3 Comparativo de las estructuras de la Leyes de Datos Personales [3], [4], [5].

Además, las leyes de ambos países establecen una serie de derechos con los que se busca garantizar a las personas el control sobre sus datos personales. La Tabla 4 muestra el resumen de dichos derechos:

	Ecuador	**México**	
	LOPDP	**LFPDPPP**	**LFPDPPSO**
Derechos de los titulares de datos personales	• Información • Acceso • Rectificación y actualización • Eliminación • Oposición • Portabilidad • Suspensión de tratamiento • A no ser objeto de una decisión basada en	• Acceso • Rectificación • Cancelación • Oposición	• Acceso • Rectificación • Cancelación • Oposición

	valoraciones automatizadas. • Consulta • Educación digital		

Tabla 4. Derechos establecidos en cada Ley [3], [4], [5].

4.2.2 Términos y definiciones relevantes

La inclusión de términos y definiciones dentro de una ley es fundamental porque evita ambigüedades, facilita el cumplimiento, protege los derechos de las partes afectadas y promueve la transparencia. La Tabla 5 permite comparar algunos de los términos relevantes en cada Ley.

	Ecuador	**México**	
Términos	**LOPDP**	**LFPDPPP**	**LFPDPPSO**
Consentimiento	"Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos"	"Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos."	"Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;"
Datos Personales	"Dato que identifica o hace identificable a una persona natural, directa o indirectamente."	"Cualquier información concerniente a una persona física identificada o Identificable"	"Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a

			través de cualquier información”
Datos Personales sensibles	“Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales”	“Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.”	“Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual”
Disociación	“Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se	“El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.”	“El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo”

	atribuyan a una persona física identificada o identificable.”		
Encargado	“Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales”	“La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.”	“La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable”
Responsable	“Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.”	“Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.”	“Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales”
Titular	“Persona natural cuyos datos son objeto de tratamiento.”	“La persona física a quien corresponden los datos personales”	“La persona física a quien corresponden los datos personales”
Tratamiento	“Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención,	“La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.”	“Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización,

	registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.“		conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales”

Tabla 5. Comparativa en la definición de términos relevantes en cada ley [3], [4], [5].

Se considera conveniente señalar que existe mayor similitud entre las definiciones de la LOPDP de Ecuador y la LGPDPPSO de México, en contraste a la LFPDPPP. Esto se debe a que estas dos últimas leyes han adecuado más su norma con la del Estándar Iberoamericano.

4.2.3 Código Penal y otras Leyes

El sistema de regulación jurídica, al incorporar los principios y postulados del derecho penal en relación con el uso ilícito de la informática y las Tecnologías de la Información y Comunicación (TIC), tiene como objetivo principal proporcionar seguridad jurídica a los usuarios, tanto públicos como privados en lo que concierne a bienes jurídicos informáticos, entre los que se pueden incluir: datos personales, propiedad intelectual, privacidad, derechos digitales, entre otros.

El Convenio sobre el Ciberdelito, conocido también como el "Convenio de Budapest" creado en el año 2001 [35], se destaca hasta la fecha como la normativa internacional más completa y sostiene que el combate contra la ciberdelincuencia demanda una cooperación internacional robusta, ágil y efectiva en el ámbito legal.

Este tratado sirve como modelo para países interesados en desarrollar una legislación nacional integral sobre ciberdelitos, entre las cuales se incluye la adaptación del marco jurídico para abordar las siguientes cuatro categorías de infracciones:

- Categoría 1: Infracciones contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos que pueden manifestarse mediante el acceso no autorizado, la interceptación ilegal, ataques contra la integridad de los datos y el funcionamiento del sistema, uso indebido de dispositivos y equipos.
- Categoría 2: Delitos de falsificación y fraude informático como parte de los Delitos Informáticos.
- Categoría 3: Delitos relacionados con el contenido, centrándose en conductas referentes con la pornografía infantil.
- Categoría 4: Infracciones vinculadas a las violaciones de la propiedad intelectual y derechos conexos.

EN ECUADOR

El Código Orgánico Integral Penal (COIP) tiene la finalidad de regular la autoridad sancionatoria del Estado, definir las conductas delictivas y garantizar el respeto al debido proceso.

El COIP tipifica y sanciona los siguientes delitos informáticos (ver Tabla 6):

Normativa	Categoría	Delito	Pena Privativa de Libertad
Código Orgánico Integral	Acceso no autorizado, interceptación,	Art. 234 "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones."	De 3 a 5 años

	ataques a la integridad.	Art. 230 “Interceptación ilegal de datos.”	De 3 a 5 años
		Art. 229 “Revelación ilegal de base de datos.”	De 1 a 3 años
		Art. 232 “Ataque a la integridad de sistemas informáticos.”	De 3 a 5 años
		Art. 233 “Delitos contra la información pública reservada legalmente.”	De 5 a 7 años
	Falsificación y fraude	Art. 234.1 “Falsificación informática”	De 3 a 5 años
		Art. 231 “Transferencia electrónica de activo patrimonial.”	De 3 a 5 años
		Art. 190 “Apropiación fraudulenta por medios electrónicos”	De 1 a 3 años
		Art. 191 “Reprogramación o modificación de información de equipos terminales móviles”	De 1 a 3 años
		Art. 230.2 y 230.3 “Interceptación ilegal de datos”	De 3 a 5 años
	Pornografía Infantil	Art. 103 “Pornografía con utilización de niñas, niños o adolescentes”	De 13 a 17 años
		Art. 104 “Comercialización de pornografía con utilización de niñas, niños o adolescentes”	De 10 a 13 años
		Art. 178 “Violación a la intimidad”	De 1 a 3 años
		Art. 179 “Revelación de secreto o información personal de terceros”	De 1 a 3 años
	Propiedad Intelectual	Art. 208 B “Actos lesivos a los derechos de autor”	De 6 meses a 1 año y Multa de 8 hasta 300 SBU (Salarios Básicos Unificados)

Tabla 6. Delitos Informáticos tipificados en el Código Integral Penal de Ecuador [30].

Nota.: El Salario Básico Unificado en Ecuador para el año 2023 es de US$ 450,00 dólares de los Estados Unidos de América mensuales [36].

EN MÉXICO

La creciente informatización de la sociedad y la proliferación de actividades ilícitas en el ciberespacio han generado una demanda global para la actualización de los marcos legales. Esto implica reformar las hipótesis jurídicas existentes y crear nuevas categorías de conductas criminales relacionadas con el uso de la informática (ver Tabla 7).

Normativa	Categoría	Delito	Pena Privativa de Libertad	Multa económica
Código Penal Federal	Acceso no autorizado, interceptación, ataques a la integridad.	Art. 211 Bis 1, párrafo segundo "Al que sin autorización conozca o copie información contenida en sistemas."	De 3 meses a 1 año	De 50 a 150 días de salario
		Art. 211 Bis 2, párrafo tercero "Al que sin autorización conozca o copie información contenida en sistemas de seguridad pública."	De 4 a 10 años	De 500 a 1000 días de salario
		Art. 211 Bis 3, párrafo segundo y tercero	De 1 a 4 años	De 150 a 450 días de salario
		Art. 211 Bis 4, párrafo segundo	De 4 a 10 años	De 500 a 1000 días de salario
		Art. 211 Bis 5, párrafo segundo	De 3 meses a 2 años	De 150 a 300 días de salario
		Art. 167 fracción VI "Al que dolosamente interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica…"	De 1 a 5 años	De 100 a 10.000 días de salario

		Art. 168 Bis fracción I "Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas…"	De 6 meses a 2 años	De 300 a 3000 días de salario
		Art. 426 fracción II "A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite…"	De 6 meses a 4 años	De 300 a 3000 días de salario
Ley de Instituciones de Crédito		Art. 113 bis 2 inciso b "Permitan que los funcionarios o empleados de la institución de crédito alteren o modifiquen registros …"	De 3 a 9 años	De 30000 a 300000 días de salario
Ley de Mercado de Valores		Art. 376 fracciones IV y V "Destruyan u ordenen se destruyan total o parcial información con el propósito de impedir actos de supervisión …"	De 2 a 10 años	
Código Penal Federal	Falsificación y fraude	Art. 231 fracción XIV "A quien por cualquier medio accese, entre o se introduzca a los sistemas informáticos e indebidamente realice movimientos de dinero …"	De 4 meses a 11 años. (Depende del monto del perjuicio económico)	De 25 a 1200 días multa
	Pornografía Infantil	Art. 187 Al que promueva a un menor de 18 años a realizar actos sexuales para describirlos a través de sistemas de cómputo, electrónicos.	De 7 a 14 años	De 2500 a 5000 días multa
		Art. 187 Al que almacene para si o para un tercero material pornográfico …	De 1 a 5 años	De 100 a 500 días multa

		Art. 202 “Delito de pornografía de personas menores de dieciocho años de edad …”	De 7 a 12 años	De 800 a 2000 días multa
		Art. 202 bis y 2023“Quien almacene material pornográfico …”	DE 1 a 5 años	De 100 a 500 días multa
	Propiedad Intelectual	Art. 424 bis fracción I “A quien reproduzca, almacene videogramas o libros protegidos por Ley Federal del Derecho de Autor	De 3 a 10 años	De 2000 a 20000 día multa
		Art. 424 bis fracción II “A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación”	De 3 a 10 años	De 2000 a 20000 día multa
		Art. 426 fracción II “A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal”	De 6 meses a 4 años	De 300 a 3000 días multa

Tabla 7. Delitos Informáticos tipificados en el Código Penal Federal de México [37], [38], [39] .

Nota.: Salario mínimo en México para el año 2023 es de $207,44 pesos diarios [40].

En México, la entidad encargada de garantizar la protección de la información es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Este organismo autónomo tiene la responsabilidad de fomentar y divulgar los derechos al acceso a datos públicos y a la salvaguardia de datos tanto en entidades públicas y privadas. El INAI se compromete a colaborar estrechamente

con las autoridades con el objetivo de promover la protección de la información. En todos los procedimientos relacionados con la protección de datos. El INAI actuará como primera instancia, y sus decisiones estarán sujetas a posibles recursos legales ante los Tribunales Judiciales Federales

4.3 Resultado del análisis comparativo

En esta sección se resaltarán las similitudes y diferencias más relevantes entre las leyes de protección de datos personales de Ecuador y México.

En cuanto a las similitudes, se destaca que ambos países tienen como finalidad establecer principios que garanticen el derecho de las personas a la protección de sus datos y privacidad. Ambos marcos normativos regulan que el tratamiento de esta información sea realizado de manera legal, consentida e informada, otorgando simultáneamente derechos a los titulares de datos para garantizar un control efectivo sobre su información personal.

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) y en México, tanto la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), reconocen y garantizan los derechos ARCO[1] de los titulares de datos. Estos derechos comprenden el acceso a la información personal, la rectificación de datos inexactos, la cancelación de datos innecesarios y la capacidad de oponerse al tratamiento de datos bajo circunstancias específicas.

Las leyes de ambos países requieren que los responsables del tratamiento de datos personales cumplan con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y confidencialidad.

[1] Son el conjunto de derechos diseñados para asegurar a las personas el control sobre sus datos personales. (**A**cceso, **R**ectificación, **C**ancelación, **O**posición).

Una entidad de supervisión con independencia y mecanismos apropiados es crucial para garantizar la implementación de la Ley. En Ecuador, La LOPDP señala que la Superintendencia de Protección de Datos será la autoridad encargada de supervisar y hacer cumplir la Ley; sin embargo, cabe mencionar que esta Autoridad de Protección aún está pendiente de creación en Ecuador (hasta la fecha de culminación de este trabajo). En contraste, en México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) actúa como la entidad reguladora para tanto la LFPDPPP como la LGPDPPSO.

Además, ambas leyes imponen responsabilidades específicas a los encargados y responsables de tratamiento de datos personales, delineando quiénes son los sujetos obligados y los estándares de cumplimiento, con especial énfasis en la seguridad de la información.

Si bien existen similitudes destacables, como los derechos ARCO, también existen diferencias importantes entre las que podemos mencionar:

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece reglas tanto para el sector público y privado. Por el contrario, en México, para el sector privado existe la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), mientras que en el sector público está la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) regula a los organismos estatales.

En Ecuador, la LOPDP define datos personales como cualquier dato vinculado a una persona natural identificada o identificable, directa o indirectamente. Esto es coherente con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que ha influido en muchas legislaciones. Sin embargo, en México, la LFPDPPP coincide parcialmente, considerando los datos personales como cualquier información que identifique o haga identificable a una persona física, no obstante, no señala la forma en que se puede identificar a la persona, directa o indirecta.

En Ecuador, se hace una diferenciación en la forma en que se tratan los datos personales, la LOPDP dedica un capítulo a la definición de categorías especiales de

datos personales, como son los datos sensibles; la información sobre niños, niñas y adolescentes, los datos relativos a la salud; así como los datos concernientes a personas con discapacidad y sus representantes legales. La gestión de estas categorías especiales de datos personales requiere el cumplimiento de requisitos específicos, como obtener el consentimiento y la necesidad de que dicho consentimiento sea explícito. En contraste, la LFPDPPP no define consideraciones especiales para los datos de niños, niñas y adolescentes y personas con discapacidad.

Con relación al consentimiento para el tratamiento de datos personales, ambos países determinan que la manifestación requiere ser: libre, específica, informada e inequívoca. La LGPDPPSO de México incluye 2 características adicionales, que el consentimiento debe ser previo y expresa (voluntad manifiesta del titular) o tácita (titular no manifieste voluntad en sentido contrario). Al respecto, la LOPDP de Ecuador no incluye estas dos características, y por el contario plantea dos momentos para proporcionar el consentimiento: 1) cuando el responsable tenga una aproximación con el propietario de la información; y 2) con carácter excepcional cuando los datos no fueron obtenidos directamente del titular y sucede después de la recopilación. Esto plantea un desafío, ya que, aunque se requiere un consentimiento inequívoco, la ley no establece un estándar claro de cómo debe ser esta manifestación.

Con respecto al delegado de Protección de Datos (DPD), la LOPDP de Ecuador establece que debe ser una persona natural encargada de informar al responsable o encargado sobre las obligaciones legales en materia de datos personales, así también determina cuando una organización está obligada a contar con DPD, pudiendo la Autoridad de Datos Personales establecer nuevas circunstancias que requieran la designación de un delegado de protección de datos personales. En este sentido, proporcionará pautas adecuadas para llevar a cabo dicha designación. Por otra parte, en México se conoce como Oficial de Protección de Datos Personales, y a diferencia de Ecuador, su figura es opcional. No obstante, su función es esencial para prevenir los impactos mal uso de información y violaciones de seguridad.

El sistema de sanciones establecido por la LOPDP de Ecuador ha categorizado las infracciones en dos niveles: leves y graves. Las infracciones leves se definen con una multa que oscila entre el 0.1% y el 0.7%, calculada sobre el volumen de negocio correspondiente al ejercicio económico anterior al momento de la imposición de la multa para el sector privado y de 1 a 10 Salarios Básicos Unificados (SBU) para el sector público. En cambio, las infracciones graves conllevan una multa que va del 0.7% al 1% del volumen de negocio correspondiente al ejercicio económico anterior para el sector privado y de 10 a 20 Salarios Básicos Unificados (SBU) para el sector público. Por su parte, en México la LGPDPPSO se imponen medidas de apremio que van desde los 150 a 1500 veces el valor diario de la Unidad de Medida y Actualización (UMA) [41].

Nota.: El valor de la UMA en México para el año 2023 es de $103,74 pesos diarios y se utiliza para calcular multas, impuestos y trámites gubernamentales [41].

4.4 Desafíos en la Protección de Datos

La entrada en vigor de una ley trae consigo una serie de obstáculos y dificultades que afectan tanto a las organizaciones como a las personas cuya información se procesa. Lograr que las instituciones tanto públicas como privadas logren una implementación correcta de los mecanismos normativos en materia de protección de datos personales es esencial e implica un cambio y fortalecimiento de la cultura organizacional que permita afrontar amenazas cibernéticas y vulnerabilidades.

Sensibilizar al personal a cargo del tratamiento de datos personales sobre la importancia de proteger los datos personales. Este esfuerzo busca minimizar el riesgo de incumplimiento o la aplicación parcial de los criterios de protección establecidos en la Ley de ambos países.

Garantizar que tanto las entidades públicas como privadas realicen de manera oportuna la solicitud y asignación de recursos necesarios, con el propósito de prevenir que la escasez de recursos sea un impedimento para cumplir la ley.

Asegurar que la población perciba de forma efectiva la protección de sus datos personales. Las personas deben confiar que el Estado garantiza sus derechos y protege su privacidad. Para esto, es necesario que la personas cuenten con herramientas tecnológicas para acceder y disponer de sus datos personales en cualquier momento y lugar; estas herramientas pueden ser: aplicaciones móviles para la consulta de datos personales, sistemas de notificación vía correo electrónico que informen a los titulares cuando sus datos están siendo tratados, portales web para quejas, publicación de informes de transparencia por parte de las empresas que tratan datos personales.

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

Para la implementación de un Sistema de Gestión de Seguridad de la Información que permita superar los desafíos expuestos en el capítulo anterior y garantizar la seguridad de los datos personales de los ciudadanos, se debe hacer uso de estándares internacionales que brinden las mejores prácticas para su implementación, de tal forma que se pueda minimizar riesgos de los activos de información, prevenir y tratar las diferentes amenazas y vulnerabilidades en el menor tiempo posible, cuidando que se cumplan con los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [42].

Para la implementación de un SGSI de datos personales se debe considerar:

5.1 Definir el Alcance y los Objetivos

En el alcance del SGSI se debe limitar el entorno de aplicación que incluya todos los datos personales a los que se da tratamiento dentro de la organización, tanto en medios físicos o medios electrónicos y en él se debe tener en cuenta:

1. Origen de los datos personales (titular, fuente pública, transferencia o comunicación, entre otros.
2. Identificación de las organizaciones o departamentos que procesan datos personales en función de sus actividades.
3. Identificación del personal autorizado para procesar datos personales.
4. Finalidad del procesamiento de datos personales.
5. Destinatarios y propósitos de las transferencias de datos personales.
6. Procedimiento para el almacenamiento de datos personales (ubicación, frecuencia, medios utilizados).
7. Mecanismos utilizados para el procesamiento de datos personales.

8. Período de tiempo durante el cual se almacenan los datos personales.
9. Instrucciones para la eliminación y destrucción de datos personales.

Por otra parte, al momento de establecer los objetivos se debe tener presente que los mismos sean reales y cuantificables, con el fin de permitir un tratamiento de datos personales que sea legal y controlado. En el establecimiento de estos objetivos, es importante considerar los siguientes aspectos:

1. Reducir la cantidad de vulneraciones a los datos personales en comparación con registros previos. Si no existen registros previos, es posible obtener esta información mediante un análisis de riesgos.
2. Minimizar la cantidad de personas que tienen acceso a los datos personales dentro de la organización. Esta información también se puede obtener durante el análisis de riesgos.
3. Evaluar los recursos tecnológicos disponibles en el mercado y determinar cuáles son adecuados para el tratamiento de datos personales en la organización.

5.2 Elaborar la Política de Seguridad de Datos personales

Esta política tiene como objetivo principal asegurar que la información personal de los titulares, como nombres, direcciones, números de identificación, información financiera, se gestione de manera segura y de acuerdo con las leyes y regulaciones de protección de datos vigentes.

Es fundamental que este documento contenga reglas claras y específicas, así como establecer las responsabilidades de cada uno de los empleados en la protección de los datos personales. y evitar que las amenazas impacten significativamente. Las políticas deben ser revisadas de forma periódica y actualizadas de ser necesario.

Es necesario que las políticas de seguridad se revisen y actualicen regularmente para asegurar su relevancia y eficacia. Es importante que la alta gerencia demuestre su compromiso con el cumplimiento de estas políticas.

Para su efectiva implementación, las políticas de seguridad deben ser socializadas entre todos los empleados de la organización. El departamento de sistemas tiene la responsabilidad de realizar este proceso de manera adecuada, a través de circulares, correos electrónicos, intranet y procesos de capacitación y concientización.

Cada usuario es responsable de cumplir con las reglas establecidas en la política de seguridad y debe ser consciente de su importancia en la protección de los datos personales de la organización.

5.3 Roles y obligaciones de las personas que dan tratamiento a los datos personales

El responsable o encargado del tratamiento de datos personales documentará los roles, responsabilidades y la rendición de cuenta de las personas que traten datos personales dentro de la organización, entendiéndose el tratamiento como cualquier operación o uso de datos personales.

Se debe hacer uso de matrices que de forma clara y precisa permita identificar quién y qué tipo de tratamiento se da a los Datos Personales.

El responsable del Tratamiento de Datos personales debe revisar, supervisar y documentar lo establecido en la matriz de roles y responsabilidades.

En la Tabla 8 se puede observar un ejemplo de las principales operaciones que se realizan con los datos personales, y cuáles son los cargos de los funcionarios responsables de este tratamiento.

Tratamiento (Datos Personales)	Jefe de Servicio al Cliente	Jefe de Cobranzas	Jefe de Sistemas	Responsable Tratamiento de Datos Personales
Recogida	X		X	
Recopilación		X	X	
Registro	X		X	
Conservación			X	
Custodia			X	
Modificación	X	X		
Eliminación			X	
Consulta		X	X	
Posesión			X	
Distribución		X		
Transferencia		X		

Tabla 8. Matriz de roles y responsabilidades de personas que tratan datos personales [43].

En la Tabla 9 se puede observar como todos los funcionarios que den tratamiento a datos personales, sin perjuicio del cargo que desempeñen tienen la obligatoriedad de informar al responsable del Tratamiento de Datos Personales, y éste a su vez, debe rendir cuentas tanto al Titular como a la Autoridad de Protección de Datos Personales.

Tratamiento (Datos Personales)	Jefe de Servicio al Cliente	Jefe de Cobranzas	Jefe de Sistemas	Responsable Tratamiento de Datos Personales	Titular	Autoridad de Protección de Datos Personales
Jefe de Servicio al Cliente		X		X		
Jefe de Cobranzas				X		
Jefe de Sistemas				X		

Responsable Tratamiento de Datos Personales					X	X

Tabla 9. Matriz de rendición de cuentas [43].

Todas las personas involucradas en el SGSI para el tratamiento de datos personales deben conocer sus funciones y en que parte se encuentra involucrado para el cumplimiento de los objetivos del SGSI, así como las consecuencias de su incumplimiento.

Actividades	Directores	Responsable Tratamiento de Datos Personales	Jefe de Sistemas
Políticas y Objetivos del SGSI para el tratamiento de datos personales	X		X
Funciones y obligaciones		X	X
Inventario de Datos Personales	X		X
Análisis de riesgo de los datos personales		X	X
Análisis de brecha y Plan de Trabajo	X		X
Implementación de medidas de Seguridad correspondientes a los datos personales			
Revisión y Auditoría	X		X
Mejora continua y capacitación a empleados			X

Tabla 10. Matriz de actividades dentro del SGSI [43].

5.4 Inventario de Datos Personales

Es fundamental realizar un inventario de todos los datos personales con los que cuenta la organización, tanto físicos como digitales, así como identificar la finalidad con la que estos datos personales fueron recabados.

Al momento de levantar el inventario es importante conocer el tratamiento que se da a los datos personales, el mismo que obligatoriamente debe abarcar todo el ciclo de vida, desde que se recoge, almacena, trata, procesa, cede, transfiere y se elimina [4].

En la Tabla 11 se puede observar un ejemplo de formato de inventario para levantar información de quienes estarán a cargo del tratamiento de los datos personales. Este formato de inventario se debe enviar a los Directores, Jefes Departamentales, Administrador de la Base de Datos, Oficiales de Crédito, entre otros.

<table>
<tr><td>Nombre del Departamento:</td><td colspan="2">Secretaría General</td></tr>
<tr><td>Nombre del Sistema:</td><td colspan="2">Sistema de Digitalización</td></tr>
<tr><td>Datos personales que contiene el sistema:</td><td colspan="2">Nombres completos, número de cédula, dirección domiciliaria, número de teléfono, correo electrónico, imagen de cédula y certificado de votación</td></tr>
<tr><td>¿Cómo se captan los datos personales?</td><td colspan="2">Físico ☒ Digital ☐</td></tr>
<tr><td>¿Para qué se utilizan?</td><td colspan="2">Para el registro de solicitudes a la Máxima Autoridad Institucional</td></tr>
<tr><td rowspan="3">¿Los datos personales se comparten?</td><td colspan="2">SI ☒ NO ☐</td></tr>
<tr><td>¿Con quienes se comparte?</td><td>¿Para qué se comparte?</td></tr>
<tr><td>Gobierno ☒
Departamento interno ☒
Departamento externo ☐</td><td>Par revisión de Procuraduría Síndica y Departamento Jurídico.</td></tr>
<tr><td>¿Dónde se encuentran almacenados los datos personales?</td><td colspan="2">Computador: De la empresa ☒ Personal ☐
Servidor: ☒
Correo electrónico: Institucional ☒ Personal ☒
Nube: ☐
Otros _____</td></tr>
<tr><td>¿Durante que tiempo se da tratamiento a los datos personales?</td><td colspan="2">Desde que se recibe la documentación en ventanilla y hasta que se comparte con el Departamento Jurídico.</td></tr>
<tr><td colspan="3">Responsable:</td></tr>
<tr><td>Nombre:</td><td colspan="2">Juan Delgado Zavala</td></tr>
<tr><td>Cargo:</td><td colspan="2">Secretaria Técnica</td></tr>
<tr><td>Funciones:</td><td colspan="2">Recoge, procesa y comparte datos personales</td></tr>
<tr><td>Obligaciones:</td><td colspan="2">Mantener la confidencial de los datos personales</td></tr>
<tr><td colspan="3">Encargado:</td></tr>
<tr><td>Nombre:</td><td colspan="2">No aplica</td></tr>
<tr><td>Cargo:</td><td colspan="2">No aplica</td></tr>
</table>

Funciones:	No aplica
Obligaciones:	No aplica

Tabla 11. Ejemplo Formato Inventario para quienes tratan datos personales [43].

5.5 Análisis de Riesgos de Datos Personales

El análisis de riesgos es una herramienta que permite identificar los principales riesgos que enfrenta una organización, tales como desastres naturales, fallas a nivel de infraestructura, fallas humanas, entre otro. Así mismo, permite priorizar medidas para minimizar la probabilidad que se materialice un riesgo, o el impacto en la organización en el caso de que dicho riesgo se materialice.

Por tanto, previo a la implementación de un SGSI resulta importante elegir la metodología que más se ajuste a la organización, estimando los recursos financieros, la capacitación del personal con que se cuenta y el tiempo disponible. Entre las metodologías disponibles para el análisis de riesgos se encuentran: CRAMM, MAGERIT, NIST SP 800-30, ISO/IEC 27001 [44].

5.6 Establecer Análisis de Brecha y Medidas de Seguridad

Análisis de brecha

El análisis de brecha permite comparar el estado actual de la organización con los requisitos establecidos en la Ley de Datos, lo que permite a la organización tomar medidas para cerrar esas brechas y garantizar el cumplimiento de la ley. La identificación de brechas permite también determinar cuáles son las medidas de

seguridad que deben implementarse para fortalecer la protección de los datos personales.

Medidas de seguridad

Las medidas de seguridad relacionadas principalmente a la Protección de Datos personales tienen como principal propósito el prevenir que exista la pérdida, alteración, destrucción, divulgamiento o tratamiento no autorizado de las actividades relacionadas con la confidencialidad de los datos que puedan vulnerar a los titulares de los datos [45].

Para cumplir con este propósito se recomienda implementar al menos 3 tipos de medidas de seguridad: administrativas, físicas y técnicas.

Medidas de seguridad administrativas

1. Acuerdo de confidencialidad: Es importante que todo el personal que realice tratamiento de datos personales debe estar plenamente informado de sus deberes y obligaciones relacionados a las medidas de seguridad, para lo cual se sugiere que firmen un acuerdo o contrato de confidencialidad y no divulgación de los datos personales. Este acuerdo debería ser de plazo indefinido desde la firma del contrato laboral y mantenerse, aunque el funcionario sea desvinculado de la organización.
2. Lista de empleados: Es esencial llevar un registro del personal que trata datos personales. Este registro debe incluir al menos, el nombre del funcionario, cargo, nivel de acceso y tipo de tratamiento que realiza sobre los datos personales. Este registro se debe llevar por cada tratamiento que se realice sobre los datos personales.
3. Capacitación continua: Todo el personal que realice el tratamiento de datos personales debe asistir de forma obligatoria a cursos y seminarios organizados por la empresa. Estas capacitaciones deben ser periódicas y actualizadas para que el personal esté al tanto de las últimas amenazas y vulnerabilidades.
4. Transferencia: Durante la transferencia de datos personales se debe garantizar la confidencialidad. Si los archivos son físicos deberán transferirse

en un sobre cerrado con una inscripción que tenga una etiqueta que indique su importancia (por ejemplo: “Confidencial”). Si son archivos electrónicos, se deben transferir encriptados. Además, se recomienda que solo se transfieran datos personales a terceros que hayan firmado un acuerdo de confidencialidad y que estén sujetos a las mismas medidas de seguridad de la empresa.

Medidas de seguridad físicas:

1. Control de acceso: El acceso a los equipos informáticos y los archivadores que contienen datos personales debe ser restringido únicamente al personal autorizado e identificado según su perfil. Se debe llevar un registro de acceso y controlar el tratamiento que se realiza a los datos.
2. Protección de equipos informáticos: Los equipos informáticos propiedad de la empresa deben ser utilizados exclusivamente con el software autorizado y no deben ser modificados sin la autorización del área de Tecnología. Además, no se deben instalar equipos informáticos que no sean propiedad de la empresa y el área de Tecnología debe implementar mecanismos de seguridad para evitar que equipos ajenos a la institución puedan obtener una dirección IP válida.
3. Protección de archivos físicos: Los archivadores que contienen datos personales deben ser asegurados con candado o llave de seguridad, y los equipos informáticos que contienen bases de datos personales también deben ser asegurados.
4. Identificación del personal: El personal autorizado y asignado a la recepción de datos personales debe portar en todo momento una credencial que lo identifique, la misma debe contener fotografía actualizada, nombres completos y departamento al que pertenece.
5. Zona segura: Se debe asignar una zona para la recepción de datos personales, la misma que deberá contar con infraestructura apropiada que permita mantener los datos de forma segura y organizada. Dentro de la zona segura están prohibidos computadores y equipos tecnológicos personales, equipos

de copiado, así como unidades de almacenamiento externos.

Medidas de seguridad técnicas

1. Contraseña: Para garantizar la seguridad de la información, se establece que la contraseña de acceso a la red, correo electrónico, equipos tecnológicos o cualquier recurso provisto por la empresa es de uso personal e intransferible. Es importante que la contraseña sea robusta y actualizada de forma periódica al menos dos veces al año. Para ello se sugiere seguir los siguientes criterios:

    - La longitud de la contraseña debe ser de al menos 12 caracteres.
    - No debe contener el nombre o apellidos del usuario.
    - Debe contener al menos una letra mayúscula, una minúscula, un número y un caracter especial.
    - No se permiten contraseñas que hayan sido utilizadas anteriormente.

2. Reporte de fallas: Para mantener la seguridad de los sistemas informáticos de la empresa se establece la obligación de notificar al área asignada cualquier tipo de falla, error o violación de seguridad. Queda prohibido hacer pruebas y buscar fallas en los sistemas informáticos de la empresa.
3. Instalación de software: Para evitar posibles riesgos de seguridad, está prohibido descargar e instalar software no autorizado en los equipos informáticos de la empresa.

5.7 Implementación de medidas de seguridad

La implementación de medidas de seguridad eficaces en la empresa requiere una visión clara de los riesgos potenciales y la identificación precisa de indicadores clave. Estos indicadores proporcionan información esencial para la toma de decisiones efectivas en lo que respecta a la protección de datos personales y para diseñar estrategias de seguridad proactivas que resguarden la confidencialidad, integridad y disponibilidad de los datos.

Para asegurar el cumplimiento de la Ley Orgánica de Protección de Datos Personales, es necesario designar un responsable de datos personales dentro de la empresa, quien tendrá entre sus principales responsabilidades:

1. Garantizar el cumplimiento de las políticas de seguridad.
2. Informar a los titulares de los datos sobre su tratamiento dentro de la empresa.
3. Implementar las mejores prácticas de seguridad según el volumen de datos personales.
4. Definir procesos que permitan verificar, evaluar y valorar de forma continua las medidas implementadas para garantizar el tratamiento de los datos personales.
5. Asegurar los datos personales en caso de transferencia fuera de la empresa.
6. Revisar y aprobar los procedimientos que involucren el tratamiento de datos personales como los requerimientos de los titulares, los tratamientos de datos personales y la gestión de reclamos.

De forma general se pueden considerar cuatro formas principales de tratar el riesgo: mitigación, retención, evitación y transferencia.

Mitigación el riesgo

La mitigación del riesgo consiste en implementar medidas y controles adecuados que proporcionen diferentes tipos de protección como prevención, eliminación, minimización, disuasión, recuperación, concienciación, asociados al tratamiento de datos personales.

Para mitigar el riesgo pueden tomarse en cuenta las siguientes acciones:

1. Implementar medidas de seguridad: Para reducir el riesgo de accesos no autorizados a datos personales, se puede cifrar los datos, uso de contraseñas

seguras, autenticación de usuarios, gestión de acceso, permisos y monitoreo al sistema.

2. Establecer políticas claras de seguridad: Se deben definir las responsabilidades y los roles de los empleados que realizan tratamiento de los datos personales.
3. Capacitar a los empleados: Los empleados deben ser conscientes de la importancia de mantener protegidos los datos y de la participación que tienen durante la mitigación del riesgo. Estas capacitaciones deben incluir el uso de buenas prácticas de seguridad, conocimiento de las políticas y procedimientos de seguridad implementadas en la organización.
4. Realizar evaluación de riesgo: Evaluar los riesgos periódicamente permite identificar los riesgos emergentes y establecer medidas de seguridad adicionales para mitigarlos.

Durante el proceso de selección de medidas y controles, es importante tener en cuenta los costos de adquisición, implementación, monitoreo y mantenimiento, en comparación con los valores de los objetivos que se buscan proteger. Además, se debe considerar el tiempo necesario para implementar los controles, así como las características técnicas y ambientales relevantes.

Los responsables de seleccionar los controles deben asegurarse de que las soluciones garanticen la seguridad de los datos personales, y sin crear una sensación de seguridad que pueda llevar a un aumento del riesgo en lugar de reducirlo.

Retención del riesgo.

Cuando se decide retener el riesgo, es importante implementar acciones que permitan asumir y controlar los riesgos de manera efectiva. A continuación, se presentan algunas acciones que se pueden tomar para retener el riesgo:

1. Definición de criterios de retención: Establecer criterios claros para determinar qué riesgos se retendrán. Esto implica definir límites aceptables de riesgo y establecer umbrales que indiquen cuándo un riesgo se considera asumible.
2. Implementación de controles internos: Poner en marcha medidas de

seguridad y controles internos para reducir la probabilidad de que los riesgos se materialicen y minimizar su impacto en caso de ocurrir.

3. Planificación de contingencias: Establecer planes de contingencia para hacer frente a los riesgos que se retienen. Estos planes deben incluir acciones específicas a tomar en caso de que ocurra un incidente, así como la asignación de responsabilidades
4. Respaldo financiero: Contar con recursos financieros suficientes para hacer frente a las consecuencias económicas de los riesgos asumidos. Esto puede implicar la asignación de presupuestos para la gestión de riesgos y la provisión de fondos para cubrir posibles pérdidas o daños.
5. Revisión y mejora continua: Realizar revisiones periódicas del enfoque de retención del riesgo y realizar ajustes o mejoras según sea necesario. Es importante estar al tanto de los cambios en las regulaciones aplicables para asegurarse de que la estrategia de retención del riesgo siga siendo efectiva y adecuada.

Cabe destacar que la decisión de retener el riesgo debe basarse en una evaluación cuidadosa y en la comprensión de los recursos y capacidades de la organización para gestionar los riesgos internamente.

Evitación del riesgo

La evitación del riesgo se basa en identificar las amenazas y vulnerabilidades potenciales que podrían afectar la seguridad de los datos. Algunas estrategias y acciones que se pueden llevar a cabo para la evitación del riesgo incluyen:

1. Eliminación de datos innecesarios: Eliminar de manera segura y permanente aquellos datos personales que no sean necesarios para la operación de la organización, reduciendo así la cantidad de información confidencial que se maneja y minimizando los riesgos asociados.
2. Restricción de acceso: Implementar controles de acceso adecuados para limitar el acceso a los datos personales únicamente a usuarios autorizados.
3. Uso de tecnologías seguras: Utilizar tecnologías y sistemas de seguridad

robustos, como firewalls, cifrado de datos y autenticación de dos factores, para proteger los datos personales contra amenazas y evitar posibles brechas de seguridad.

4. Políticas y procedimientos claros: Establecer políticas y procedimientos claros sobre el manejo y protección de datos personales.
5. Evaluación de proveedores: Realizar una evaluación de los proveedores de servicios externos que puedan tener acceso a los datos personales, garantizando que cumplan con los estándares de seguridad adecuados antes de establecer cualquier relación contractual.
6. Supervisión y auditorías regulares: Realizar auditorías periódicas y revisiones de seguridad para identificar posibles brechas y tomar acciones correctivas de manera oportuna.

La evitación del riesgo busca garantizar la protección adecuada de los datos personales, manteniendo un enfoque proactivo en la seguridad de la información.

Transferencia del riesgo.

La transferencia del riesgo implica compartir la responsabilidad de los riesgos identificados a terceros, como aseguradoras o proveedores de servicios, a través de acuerdos contractuales. Al transferir el riesgo, la organización busca minimizar su responsabilidad y mitigar los posibles impactos económicos y legales asociados.

Algunos ejemplos de acciones que se pueden llevar a cabo para transferir el riesgo son:

1. Contratos y acuerdos: Establecer contratos o acuerdos con proveedores de servicios externos que incluyan cláusulas específicas relacionadas con la responsabilidad por incidentes de seguridad y la compensación en caso de que ocurran.
2. Seguros: Obtener pólizas de seguro que cubran los riesgos relacionados con la seguridad de los datos personales. Estas pólizas pueden incluir cobertura para gastos de investigación forense, notificación a las partes afectadas, acciones legales y posibles indemnizaciones.

3. Externalización de servicios: Externalizar ciertas funciones o procesos que involucren datos personales a proveedores de servicios especializados. En este caso, la responsabilidad de la seguridad de los datos se comparte con el proveedor, quien asume parte del riesgo asociado con la gestión de la información.

Es importante tener en cuenta que la transferencia del riesgo no significa eliminar completamente la responsabilidad de la organización en la protección de los datos personales. La organización sigue siendo responsable de tomar las medidas adecuadas para evaluar y seleccionar a los proveedores externos, así como de supervisar y asegurarse de que se cumplan los acuerdos contractuales establecidos.

5.8 Revisión y auditoría

Revisión

Para la revisión se lleva a cabo una evaluación de las políticas y procesos implementados, con el fin de verificar las mejoras. Es fundamental realizar un seguimiento y evaluación continua del riesgo, considerando elementos clave, como el valor de los activos, las amenazas, las vulnerabilidades, impacto y probabilidad de ocurrencia.

Esto permitirá detectar cualquier cambio en el entorno que pueda afectar el alcance y los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización, manteniendo así una visión general actualizada de la situación de riesgo.

Estos elementos clave pueden cambiar sin previo aviso. Esta realidad implica que cada riesgo debe ser evaluado de forma individual, así como considerar su impacto acumulado potencial en conjunto con otros riesgos. Por lo tanto, es fundamental llevar a cabo un monitoreo constante para identificar estos cambios. En este contexto, resulta beneficioso contar con el respaldo de servicios externos que brinden información actualizada sobre amenazas y vulnerabilidades, lo cual facilita la identificación y gestión de los riesgos de manera más efectiva.

Las organizaciones deben garantizar el monitoreo de los siguientes aspectos:

1. Inclusión de nuevos activos en el ámbito de gestión de riesgos.
2. Modificaciones requeridas en los activos, como cambios tecnológicos.
3. Identificación de nuevas amenazas, tanto internas como externas.
4. Análisis de vulnerabilidades conocidas para determinar cuáles están expuestas a nuevas amenazas o resurgimientos de amenazas anteriores.
5. Evaluación de cambios en el impacto, vulnerabilidades y riesgos en su conjunto, que puedan resultar en un nivel de riesgo inaceptable.
6. Registro y análisis de incidentes y violaciones de seguridad.

Estos puntos deben ser objeto de un seguimiento constante para garantizar una gestión efectiva de riesgos y mantener la seguridad de la organización.

Auditoría

Es relevante contar con un programa de auditoria para monitorear y revisar el cumplimiento del SGSI.

Durante la auditoría, se deben analizar y evaluar diversos aspectos del sistema de gestión de datos personales, como:

1. Cumplimiento legal: verificar si la organización cumple con las leyes y regulaciones aplicables en materia de protección de datos personales.
2. Políticas y procedimientos: revisar las políticas y procedimientos establecidos para la gestión de datos personales, asegurando que estén documentados, actualizados y sean adecuados para proteger la privacidad de los titulares.
3. Implementación de controles de seguridad: evaluar la implementación y efectividad de los controles de seguridad físicos, técnicos y organizativos para proteger los datos personales contra accesos no autorizados, pérdida, alteración o divulgación indebida.
4. Gestión de riesgos: analizar la identificación, evaluación y gestión de los riesgos asociados al procesamiento de datos personales, asegurando que se hayan implementado medidas adecuadas para mitigar dichos riesgos.

5. Gestión de incidentes: revisar la capacidad de la organización para detectar, investigar y responder adecuadamente a incidentes de seguridad de datos personales, incluyendo la notificación oportuna a las autoridades y las partes afectadas.
6. Capacitación y concientización: evaluar si se proporciona la capacitación adecuada al personal sobre la protección de datos personales y si existe un nivel suficiente de conciencia sobre la importancia de la privacidad y la seguridad de la información.

Al finalizar la auditoría, se genera un informe detallado que incluye los hallazgos, las deficiencias identificadas y las recomendaciones para mejorar el sistema de gestión. Este informe ayuda a la organización a fortalecer su enfoque de protección de datos y cumplir con los requisitos establecidos, brindando confianza tanto a los titulares cuyos datos son procesados como a la autoridad reguladora.

5.9 Capacitaciones y mejora continua

En la fase de capacitación y mejora continua en un SGSI, se llevan a cabo diversas actividades con el objetivo de fortalecer el conocimiento y las habilidades del personal, así como mejorar constantemente el sistema de gestión. Algunas de las actividades comunes realizadas en esta fase son:

1. Capacitación en protección de datos: Se proporciona formación y entrenamiento al personal de la organización sobre los principios y requisitos de protección de datos personales, así como sobre las políticas, procedimientos y controles implementados en el SGSI. Esto ayuda a garantizar que todos los empleados comprendan su rol y responsabilidades en la protección de datos.
2. Concientización sobre seguridad de la información: Se realizan campañas de sensibilización y concientización para promover una cultura de seguridad de la información dentro de la organización. Esto implica educar a los empleados sobre las amenazas y riesgos de seguridad, así como brindar pautas y mejores prácticas para proteger los datos personales.

3. Evaluación de competencias: Se evalúa regularmente el nivel de competencia del personal en cuanto a la protección de datos personales. Esto puede incluir pruebas o evaluaciones de conocimientos y habilidades, con el fin de identificar áreas de mejora y proporcionar oportunidades de capacitación adicional si es necesario.
4. Revisión y actualización de políticas y procedimientos: Se revisan periódicamente las políticas y procedimientos del SGSI para asegurar su vigencia y eficacia. Esto implica identificar posibles brechas o áreas de mejora, y realizar ajustes o actualizaciones para mantener el sistema alineado con los cambios legales, tecnológicos o empresariales relevantes.
5. Análisis de incidentes y lecciones aprendidas: Se realizan análisis de los incidentes de seguridad o brechas de datos ocurridos, con el objetivo de identificar las causas raíz, evaluar su impacto y extraer lecciones aprendidas. Estos análisis ayudan a mejorar los controles y medidas de seguridad del SGSI, evitando la repetición de incidentes similares en el futuro.
6. Monitoreo y medición del desempeño: Se establecen indicadores clave de desempeño (KPIs) para evaluar y monitorear el funcionamiento del SGSI. Estos KPIs pueden incluir métricas como el cumplimiento de las políticas y procedimientos, la eficacia de los controles de seguridad y la respuesta a incidentes. Los resultados obtenidos permiten identificar áreas de mejora y tomar acciones correctivas o preventivas.

6 Conclusiones

En este análisis comparativo entre las Leyes de Protección de Datos Personales entre Ecuador y México, se han examinado y contrastado los marcos legales vigentes en ambos países, así como las medidas adoptadas para proteger los datos personales y prevenir los delitos informáticos. A continuación, se presentan las conclusiones obtenidas:

Tanto en Ecuador como en México, se ha reconocido la importancia de abordar los riesgos asociados a los delitos informáticos, y como resultado, se han integrado disposiciones relacionadas con la ciberseguridad en sus respectivas legislaciones, lo que demuestra su compromiso con la privacidad y la seguridad de la información.

En cuanto a la definición de datos personales, tanto Ecuador como México han establecido criterios precisos que engloban información sensible y la han categorizado según su grado de sensibilidad. Además, ambas jurisdicciones han establecido sólidos principios rectores para el tratamiento de datos personales, que incluyen el requerimiento de consentimiento informado, la especificación de finalidades, la garantía de proporcionalidad y la preservación de la confidencialidad

Es importante destacar que, en Ecuador y México, se han establecido obligaciones claras para las entidades responsables del tratamiento de datos personales. Estas responsabilidades abarcan desde la implementación de medidas de seguridad apropiadas hasta la notificación de posibles brechas de seguridad, y la designación de un encargado de protección de datos.

Adicionalmente, en ambos países, se han definido sanciones y multas en caso de incumplimiento de las disposiciones legales en materia de protección de datos

personales. Estas sanciones varían en función de la gravedad de la infracción y pueden tener implicaciones económicas significativas.

7 Glosario

Ciberataque: Es una explotación premeditada de sistemas informáticos para comprometer información y tolerar delitos.

Ciberatacante: Conocidos como piratas informáticos, son personas con fines maliciosos, generalmente podemos etiquetarlos en diferentes categorías: ciber delincuentes, ciber terroristas, ciber activistas, etc. [46]

Confidencialidad: Propiedad de información que garantiza información accesible únicamente para el autor o autorizada a terceros.

Datos personales: Considerado como documentos únicos para cada individuo. [47]

Datos sensibles: Referencia de varios campos de datos personales con información sensible presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual [48]

Ley Orgánica de Protección de Datos Personales: Protege datos personales y avala el derecho de datos propios, que encierra el acceso y disposición sobre la información, así como su conveniente protección. [4]

Privacidad: Espacio personal de un individuo, quien se desenvuelve en un espacio reservado, el cual tiene como propósito principal mantenerse confidencial.

Seguridad de datos: Medida de protección empleada contra acceso no autorizado y para resguardar la confidencialidad, la integridad y la disponibilidad de la base de datos.

Sistema de Gestión de Seguridad de la Información: Es el conjunto de políticas de administración de la información por la ISO/IEC 27001. [49]

Vulnerabilidad: Es un fallo que pone en riesgo la seguridad de la información de tal manera que comprometa la integridad y confidencialidad.

8 Referencias

[1] Comisión Económica para América Latina y el Caribe, 2021. [En línea]. Available: https://www.cepal.org/sites/default/files/publication/files/46766/S2000991_es.pdf. [Último acceso: 2022].

[2] Redacción PRIMICIAS, «Fiscalía y la estafa al Isspol,» 22 Septiembre 2020. [En línea]. Available: https://www.primicias.ec/noticias/economia/fiscalia-estafa-800-millones-isspol/. [Último acceso: Julio 2022].

[3] Ley Orgánica de Protección de Datos Personales, 2021.

[4] Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010.

[5] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017.

[6] G. Sain, «Pensamieno Penal,» Abril 2015. [En línea]. Available: https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf. [Último acceso: 08 Septiembre 2022].

[7] X. Han, «Revista del Derecho,» 28 Noviembre 2020. [En línea]. Available: https://revistasdederecho.com/wp-content/uploads/2021/09/RCHRLYPS-13-diciembre-2020-_VERSION-ENERO-2021_-27-42.pdf. [Último acceso: 15 Septiembre 2022].

[8] herjavecgroup & floridatechonline & it.ie, «Guatemalan Observatory of Computer Crime OGDI,» [En línea]. Available: https://ogdi.org/historia-del-cibercrimen. [Último acceso: 15 09 2022].

[9] «mitnicksecurity,» [En línea]. Available: https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security. [Último acceso: julio 2023].

[10] Z. O. Bello, «El derecho a la protección de datos personales desde un análisis histórico-doctrinal,» 2014. [En línea]. Available: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-69162015000200058#fn13. [Último acceso: junio 2023].

[11] A. C. Silva, Mecanismos de Control en la Protección de Datos en Europa, 2006, pp. 221-251.

[12] M. L. Gurtubay, Análisis comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea, 1994.

[13] L. Joinet, Orientaciones principales de la Ley francesa relativa a la informática, los ficheros y las libertades, 1978.

[14] I. Rostión, Sobre la Ley de Protección de la Vida Privada: La importancia de una "fuente legal" y su aplicación en las Personas Jurídicas, 2015.

[15] B. Califano, Análisis del proceso de debate de iniciativas legales sobre protección dedatos personales y sus conflictos con el derecho a la libertad de expresión. Los casos de Argentina y Ecuador, Universidad de Palermo, 2021.

[16] L. O. Pineda, La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración, Universidad Andina Simón Bolívar, 2021.

[17] A. Sweigart, Hacking secret ciphers with Python, 2013.

[18] International Organization for Standardization, «ISO,» 2005. [En línea]. Available: https://www.iso27000.es/sgsi.html. [Último acceso: junio 2023].

[19] Sistema de Información Legislativa, Ley Orgánica.

[20] «Comisión Europea,» [En línea]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es#:~:text=Los%20datos%20personales%20son%20cualquier,constituyen%20datos%20de%20car%C3%A1cter%20personal.. [Último acceso: 04 agosto 2022].

[21] Revista Científica de Ciencias Jurídicas, Criminología y Seguridad, «FISCALIA GENERAL DEL ESTADO - ECUADOR,» diciembre 2021. [En línea]. Available: https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf. [Último acceso: junio 2023].

[22] Asociate Press, «El mayor banco de Ecuador sufre un ciberataque,» 23 Mayo 2021. [En línea]. Available: https://www.vozdeamerica.com/a/mayor-banco-de-ecuador-sufre-ciberataque-/6272549.html. [Último acceso: Julio 2022].

[23] J. M. Harán, «Welivesecurity by ESET,» 14 octubre 2021. [En línea]. Available: https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/#:~:text=Si%20bien%20Banco%20Pichincha%20no,Strike%2C%20la%20cual%20suele%20ser. [Último acceso: 05 junio 2022].

[24] CNT, «PRIMICIAS,» 5 Diciembre 2021. [En línea]. Available: https://www.primicias.ec/noticias/tecnologia/los- misterios-del-ataque-que-dejo-a-cnt-sumida-en- emergencia/ - 2021. [Último acceso: Agosto 2022].

[25] Ley Orgánica de Transparencia y Acceso a la Información Pública, 2004.

[26] Ley de Derechos y Amparo del Paciente, 2006.

[27] Ley Orgánica de Salud, 2006.

[28] Constitución de la República del Ecuador, 2008.

[29] Ley Orgánica de Comunicación, Ecuador, 2013.

[30] CÓDIGO ORGÁNICO INTEGRAL PENAL, 2021.

[31] Ley Orgánica de Telecomunicaciones, 2015.

[32] Constitución Política de los Estados Unidos Mexicanos, 1917.

[33] Ley Federal de Telecomunicaciones, 1995.

[34] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2002.

[35] H. R. PIÑA LIBIÉN, «Cibercriminalidad y ciberseguridad en México,» Ius Comitialis, 2019.

[36] ACUERDO MINISTERIAL No. MDT-2022-216, 2022.

[37] Código Penal Federal, 2009.

[38] Ley de Instituciones de Crédito, 2022.

[39] LEY DEL MERCADO DE VALORES, 2010.

[40] Gobierno de México, «Gobierno de México,» 01 enero 2023. [En línea]. Available: https://www.gob.mx/stps/prensa/entran-en-vigor-salarios-minimos-2023-en-todo-el-pais?idiom=es. [Último acceso: Junio 2023].

[41] P. México, ¿Qué es la UMA y cómo se calcula? Valor en 2023, 2023.

[42] Normalización, Norma Española UNE--EN ISO/IEC 27001, Madrid, 2017.

[43] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, 2014.

[44] C. R. B. Helena Alemán Novoa, «https://hemeroteca.unad.edu.co/,» [En línea]. Available: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874. [Último acceso: 01 02 2023].

[45] Suprema Corte de Justicia de la Nación, Catálogo de Medidas de Seguridad para los tratamientos de datos personales, 2019.

[46] G. S. d. T. Rotaeche, E. P. González, A. R. Garnacho y B. R. Álvarez, «Métodos y técnicas del atacante para ocultar su identidad en la Red,» , 2009. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=3416973. [Último acceso: 18 5 2023].

[47] E. T. Leal, C. M. S. Reyna, M. L. Castillo y M. M. F. Morelos, «Análisis de los servicios de la tecnología Web 2.0 aplicados a la educación,» , 2010. [En línea]. Available: http://nosolousabilidad.com/articulos/tecnologia_educacion.htm. [Último acceso: 18 5 2023].

[48] L. . Ornelas y C. G. Gregorio, «Protección de datos personales en las redes sociales digitales : en particular de niños y adolescentes,» , 2011. [En línea]. Available: http://inicio.ifai.org.mx/publicaciones/proteccionredessociales.pdf. [Último acceso: 18 5 2023].

[49] G. B. Maldonado y J. A. O. Cano, «Metodología de la seguridad de la información como medida de protección en pequeñas empresas,» , 2014. [En línea]. Available: http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202. [Último acceso: 18 5 2023].