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 URUGUAYA DESDE UN ENFOQUE DE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

AUTORES:

JANETH MARICRUZ LIMONES ZAMBRANO
JOSUE ADRIÁN PERALTA PERALTA

DIRECTOR:

MIGUEL ARTURO ARCOS ARGUDO

CUENCA – ECUADOR
2023

Autores*:*

Janeth Maricruz Limones Zambrano
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jlimones@est.ups.edu.ec

Josue Adrián Peralta Peralta
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jperaltap@est.ups.edu.ec

Dirigido por:

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

DEDICATORIA

A Dios y a mi ángel de la guarda, mi mamá, por escoltar y alumbrar mis pasos, por darme la sabiduría para culminar de manera exitosa este periodo profesional. A mi papi Segundo por ser mi superhéroe sin capa, Lisbeth y Charlie, mis increíbles hermanos, mi adorado sobrino Noah y mis espectaculares cuñados Jessenia y Jorge, por ser mi apoyo y los pilares de vida, por todo su amor y su apoyo incondicional.

Janeth Maricruz Limones Zambrano.

Toda idea se vuelve una meta por alcanzar si contamos con el convencimiento necesario de que vamos a cumplirla. Esta es una meta alcanzada que dedico a mi mamá, por ser ese amor sublime y constante, mi motor y ese ejemplo de que nada ni nadie me podrá frenar si tengo la convicción y las ganas de ser cada día mejor. A Nahim, por ser esa puesta a tierra y siempre estar para mí. Me has enseñado más de lo que yo te he podido impartir. ¡Qué sería la vida sin tu compañía! A mi papá, por todo el esfuerzo realizado y haberme dado las bases para mi vida profesional. Y, a mis abuelos, tíos, primos, mejores amigos y amigos, por ser apoyo, brindarme consejo y hacerme un espacio en sus corazones.

Con la fe intacta.

Josue Adrián Peralta Peralta.

AGRADECIMIENTO

En primero lugar a Dios, porque sin el nada fuera posible. A mi papa, mis hermanos y mis cuñados por siempre ser el soporte en cada paso que doy en mi vida.

A Josué, por compartir conmigo este sueño, por sus conocimientos y por toda la confianza depositada, este logro es de los dos.

Y, por último, pero no menos importante, a mis colegas esta maestría no hubiera sido lo mismo sin ustedes.

Janeth Maricruz Limones Zambrano.

A Dios y a la Virgen, por brindarme la sabiduría y la esperanza. A mi familia, en especial a mamá, papá y hermano por el amor infinito y el constante soporte en cada etapa y proyecto de mi vida que he llevado a cabo.

A mi hermana de la vida, Janeth, por ser cómplice en todo y terminarme de convencer que seguir esta maestría era una buena decisión.

Josue Adrián Peralta Peralta.

Tabla de Contenido

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

Autores:

Janeth Maricruz Limones Zambrano

Josue Adrián Peralta Peralta

Resumen

En el presente trabajo se realiza un análisis comparativo de la Ley Orgánica de Protección de Datos Personales en el Ecuador y la Ley 18.331 de Protección de Datos Personales de Uruguay.

Los datos personales se refieren a la información que está relacionada con aspectos personales o íntimos de una persona, y es necesario protegerlos. Sin embargo, para justificar esta protección, es importante explicar las razones por las cuales queremos resguardar esos datos personales. Al hablar de un acceso de rectificación, recolección y distribución podemos, como titulares, acceder a nuestros datos personales, pero ¿cómo se regula estos datos cuando se encuentran en manos de terceros?

Ecuador necesita contar de urgencia con una ley de protección de datos personales que regule la manera como las instituciones nacionales y extranjeras tratan, procesan, conservan y explotan comercialmente los datos personales de las personas. El país debe cumplir con estándares mínimos, para llegar a ser considerado como un país confiable para la transferencia de datos personales, lo cual permitiría el surgimiento de empresas transnacionales en Internet.

Este trabajo tiene la finalidad de analizar las similitudes jurídicas entre ambas leyes, identificar las razones o motivaciones que se tuvieron en cada país para iniciar a definir un marco legal que proteja este derecho y exponer recomendaciones que le brinden al lector, una guía y soporte durante la implementación de un Sistema de Gestión de Seguridad de la Información en cualquier organización.

Palabras clave:

Ley Orgánica de Protección de Datos Personales, Sistema de Gestión de Seguridad de la Información, Políticas de Seguridad, Ciberseguridad, Delitos Informáticos

ABSTRACT

In the present work a comparative analysis of the Organic Law of Protection of Personal Data in Ecuador and Law 18.331 of Protection of Personal Data of Uruguay is carried out.

Personal data refers to information that is related to personal or intimate aspects of an individual, and it is necessary to protect them. However, to justify this protection, it is important to explain the reasons why we want to safeguard that personal data. When talking about access to rectification, collection, distribution we can, as owners, access our personal data, but how is it regulated when these data are in third parties' hands?

Ecuador urgently needs to have a personal data protection law that regulates the way in which national and foreign institutions treat, process, preserve and commercially exploit the personal data of people. The country must comply with minimum standards, to be considered a trustworthy country for the transfer of personal data, which would allow the emergence of transnational companies on the Internet.

This work has the purpose of analyzing the legal similarities between both laws, identifying the reasons or motivations that were held in each country to begin to define a legal framework that protects this right and presenting recommendations that provide the reader with guidance and support during the implementation of an information security management system in any organization.

Key words:

Data Privacy Law, Information Security Management System, Security Policies, Cybersecurity, Cybercrime.

1 Introducción

Todo ser humano requiere sentirse protegido al entregar sus datos personales. El presente trabajo comparativo trata sobre un tema que en los últimos años ha obligado a que en diferentes países del mundo se dicten leyes sobre la protección de los datos personales. Con el avance de las Tecnologías de la Información y las Comunicaciones (TIC), surgieron aspectos que resaltaron la vulnerabilidad de los datos personales al pasar por diversas plataformas o medios electrónicos. Esto no implica que los datos personales estén exclusivamente vinculados a herramientas tecnológicas, ya que tradicionalmente también se relacionan con medios físicos como documentos. Sin embargo, se reconoce el uso de las TIC como un factor desencadenante que ha generado mayor atención en el tema que se abordará en este trabajo.

Una regulación de protección de datos personales permite que como ciudadanos podamos contar con herramientas concretas para exigir límites en el uso de la información. Ese control es esencial para garantizar nuestra libertad, autonomía y dignidad como personas, frente al Estado y las empresas, donde las desproporciones de poder y potenciales impactos en ejercicio de derechos resultan más evidentes.

Ante esta realidad, resulta preocupante el hecho de que, en el ámbito de la protección de datos, algunos países no han conseguido aún armonizar satisfactoriamente sus ordenamientos internos. La mayoría de estos, están de acuerdo en la necesidad de conciliar la libre circulación de datos con la protección del derecho a la intimidad.

Para el desarrollo de este trabajo de titulación se utilizará principalmente la metodología sistémica para realizar una investigación y revisión documental y bibliográfica con el objetivo de recopilar y examinar la información relacionada con

la ley de protección de datos del Ecuador y Uruguay. Se indagarán las estadísticas publicadas hasta la fecha actual para relacionar ventajas y desventajas de la implementación de la ley en cada país de sus leyes u órganos legales relacionados. Este trabajo tiene como objetivo hacer énfasis en el ámbito relacionado a la ciberseguridad y a los delitos informáticos. Se abordarán diversos temas desde conceptos que giran en torno al tema de estudio, la reseña histórica de la protección de datos personales tanto de Ecuador como de Uruguay, el estado de arte donde se exponen diversas opiniones sobre investigaciones acerca de la ley de protección de datos y delitos tipificados en las leyes de protección de datos de Uruguay y Ecuador.

2 Determinación del Problema

2.1 Problema

Para entender un poco más lo importante que es este movimiento para el mundo acerca de esta ley, es necesario entender la transparencia del tema que trata la Ley de Protección de Datos Personales.

Hoy, en día, los datos personales o cualquier información de una persona identificable se entregan en todas las interacciones sociales, ya sea por medio de entes privados o públicos que trabajan en todos los ámbitos de la economía, las actividades sociales y culturales.

Sin embargo, debido a la misma frecuencia y cotidianidad de procesamiento de datos personales, muchas veces exponemos demasiada información y no somos conscientes que es la puerta de entrada a nuestra vida y a nuestra capacidad de interactuar socialmente. Las normativas de protección de datos personales nos permiten como personas identificables contar con herramientas especiales para solicitar restricciones en el uso de nuestra información personal.

En virtud de la expuesto, se evidencia la importancia de realizar un análisis comparativo de la normativa ecuatoriana referente a la protección de datos personales con la legislación de otro país del entorno latinoamericano con el fin de identificar sus principales semejanzas y diferencias. Además, este análisis permitirá elaborar un conjunto de recomendaciones que los sistemas de gestión de seguridad de la información de las organizaciones ecuatorianas deben considerar al momento de su diseño e implementación, con el fin de dar cumplimiento a la norma y garantizar la seguridad de los datos de los ciudadanos.

2.2 Objetivo general

Realizar un análisis comparativo entre la Ley Orgánica de Protección de Datos Personales del Ecuador con la ley equivalente que se encuentra vigente en Uruguay, haciendo énfasis en el ámbito relacionado a la ciberseguridad y a los delitos informáticos.

2.3 Objetivos específicos

Redactar una reseña histórica sobre las necesidades que han llevado a los diferentes países a generar una ley que garantice la protección de los datos personales de los ciudadanos.

Identificar los delitos informáticos tipificados en la legislación de ambos países y diferenciar su caracterización según cada ley.

Redactar una serie de recomendaciones que se podrían considerar al momento de desarrollar un Sistema de Gestión de Seguridad de la Información para garantizar la seguridad de los datos personales de los ciudadanos según la legislación de cada país.

3 Marco teórico referencial

3.1 Reseña histórica

El derecho a la protección de datos ha experimentado importantes cambios jurídicos desde que el 10 de diciembre de 1948 en París, la Declaración Universal de los Derechos del Hombre, tuvo su primer precedente en su duodécimo artículo: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” [1].

La protección de datos personales como mecanismo de protección de la privacidad surgió en los países europeos desde finales de la década de 1970 [2]. De acuerdo con la reseña expuesta por Zamora Álvarez [2], en el año 1983 el Tribunal Constitucional de Alemania, reconoció por primera vez el término “autodeterminación informativa”. Los primeros borradores de un reglamento para la protección de datos aparecieron en 1995, cuando la Unión Europea (UE) esbozó la iniciativa de reglamentar el flujo de intercambio acelerado de los datos personales como consecuencia de la integración económica y social de los Estados miembros. Al inicio, el tratamiento de datos se administraba de forma independiente en cada país, de modo que, existían obstáculos para el tráfico transnacional de datos, es así como se implementó la primera regulación de protección de datos de la UE a través de la Directiva 95/46/CE, cuyo objetivo principal era proteger el tratamiento de los datos de las personas físicas y simultáneamente la libre circulación de los datos personales entre los Estados miembros. Fue en 1999 que se reconoció por primera vez la protección de datos personales a cargo de los organismos, agencias e instituciones de la Unión y de los Estados a través de la reforma implementada por el Tratado de Amsterdam.

Rápidamente se llegó al consenso para adicionar este derecho dentro de la Carta de los Derechos Fundamentales de la UE. Mientras tanto, en enero de 1998, el Tribunal Constitucional español reconoció que la protección de datos personales es un derecho fundamental a la circulación de la información que afecta a todos y garantiza el ejercicio de ese derecho. Asimismo, en 2014, el Tribunal de Justicia de la Unión Europea (TJUE) tomó una importante decisión analizando los datos de las comunicaciones electrónicas (metadatos) y distinguiendo entre datos simples y complejos.

Finalmente, en 2016, se aprobó el Reglamento General de Protección de Datos para llevar la regulación de protección de datos a una nueva era.

La Constitución del Ecuador [3] garantiza y reconoce en su Artículo 66 numeral 19 a las personas: “El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley”.

No obstante, previo a la publicación oficial de la Ley Orgánica de Protección de Datos Personales, no se conocía de ninguna definición específica que incluyera la comprensión de este derecho de los ecuatorianos y ecuatorianas. El único mecanismo que se tenía hasta ese momento era el habeas data.

Como presenta Guerrón Eras en su artículo [4], finalmente después de un extenuante trabajo que inicia en 2017 y que fue dirigido por la titular de la Dirección Nacional de Registro de Datos Públicos (DINARDAP), Lorena Naranjo, con la cooperación de entidades públicas, privadas y civiles, desde mayo de 2021, Ecuador implementó la primera Ley Orgánica de Protección de Datos Personales (LOPDPP), disposición que permite innovar y utilizar la tecnología, teniendo en cuenta el tratamiento de los datos personales como el eje de protección central. La LOPDPP fue promulgada el 19 de septiembre de 2019 por Lenín Moreno, Presidente de la

República del Ecuador, como una iniciativa de proyecto de ley, esto después de la noticia de la mayor filtración de datos que tuvo lugar en el Ecuador.

Los datos personales de un número considerable de ecuatorianos, incluidos menores de edad fueron expuestos en Internet a causa de una falla técnica en la base de datos de Novaestrat, descubierta por investigadores de seguridad de vpnMentor [5].

3.1.1 Delitos informáticos

Los delitos informáticos implican la intención de cometer un crimen con la ayuda de la computadora, internet, etcétera; no obstante, este tipo de delitos no se comete únicamente por estos medios, ya que son instrumentos que facilitan, pero no determinan su ejecución. El término rara vez se usa en derecho penal; sin embargo, describe una nueva forma de delincuencia que ha surgido a partir del uso generalizado de las tecnologías de la información.

Los delitos informáticos o ciberdelitos no sólo implican la comisión de hechos delictivos con la utilización de elementos o medios informáticos, o a las conductas ilícitas en las que aquellas sean su objeto, sino también a la afectación de los datos.

A continuación, se citan algunos datos importantes que Felipe Villavicencio menciona en su entrevista para la revista de la Pontificia Universidad Católica del Perú (PUCP).

De la definición de lo que es un delito informático, se entiende que no todos los delitos pueden ser tipificados como ciberdelitos por el simple hecho de haberse servido o empleado una computadora u otro dispositivo tecnológico. Al respecto, uno de los criterios a emplear seria que un posible delito informático, no sea posible de realizarse sin la intervención de la informática. Por ejemplo, el difamar a una persona a través de redes sociales, no puede establecerse como un delito informático únicamente por el hecho de emplear la tecnología como medio, pues este delito puede llevarse a cabo a través de otros medios como son verbal, escrito, etcétera. No obstante, los delitos de acceder sin autorización a un sistema o

sabotear una base de datos sí se clasificarían dentro de los delitos informativos, porque no sería posible su comisión sin la intervención de la informática [6].

Se ha mencionado que los delitos informáticos no son un nuevo tipo de delito, sino delitos similares que ya han sido sancionados: delitos contra la humanidad, la seguridad pública, el honor, la libertad. Se ha tratado de vincular los delitos informáticos con delitos comunes como: hurto, estafa, robo, falsificación, vandalismo, etcétera, pero hay que analizar si los tipos tradicionales les convienen o no [7].

¿Cuál fue el primer delito informático documentado? En 1964, el estudiante del Massachusetts Institute of Technology (MIT) Michael Dertouzos realizó los cálculos de su tesis en una de las primeras computadoras de tiempo compartido del mundo. La CPU principal estaba conectada a una pequeña cantidad de "terminales tontos" y el usuario maneja la energía y la memoria desde el procesador principal. Los administradores del campus decidieron que los profesores y personas privilegiadas tendrían la opción de usar otros dispositivos que estaban usando el sistema cuando estaba lleno. Los estudiantes de repente reciben el mensaje "Un usuario privilegiado lo ha movido" y el teclado está deshabilitado. En esta situación de "feudal información" de ricos y pobres, un desconcertado joven de 18 años hackeó silenciosamente un disco duro donde se almacenaban los nombres de usuario y los permisos. Una vez en posesión de los archivos que actuaban como contraseñas, Ben revocó los privilegios para que la gente común tuviera el poder de expulsar a las personas clave.

Estos delitos tienen muchas clasificaciones diferentes, pero en nuestra opinión es necesario tener en cuenta dos aspectos: por un lado, si la informática fue el instrumento o medio para cometer el delito; o si los sistemas informáticos fueron el fin u objetivo de estos [8].

A continuación, se citan varios de los primeros casos que se clasificaron o identificaron como delitos informáticos que han sido mencionados en la revista Seguridad 360 [9]:

Gerald Wondra fue una de las primeras personas condenadas por un delito informático. En 1983 recibió una condena de 24 meses de libertad condicional, por haber accedido sin autorización a los sistemas de entidades financieras de Estados Unidos y hacer llamadas telefónicas.

A mediados de 1994 Kevin Poulsen fue condenado a 4 años y 3 meses al ser encontrado culpable de lavado de dinero y obstrucción de la justicia con la ayuda de medios tecnológicos.

En 1995 el programador británico Christopher Pile fue condenado en el Reino Unido a 18 meses de cárcel al declararse culpable de 11 cargos que pesaban contra él entre los que constaban crear y distribuir códigos maliciosos. Dentro de los códigos maliciosos se encuentran los virus Pathogen y Queeg que se cargaban en memoria para afectar los programas que estuvieran en ejecución.

Quizá una de las condenas más famosas es la que en 1999 se le impuso a Kevin Mitnick, uno de los hackers, crackers y phreakers estadounidense más famosos de la historia y que resultó como uno de los especialistas más buscados por el FBI. Debió permanecer 68 meses en la cárcel después de ser encontrado culpable de interceptar comunicaciones y estar relacionado con otros delitos de fraude.

En 1999 Jonathan Joseph James, nativo de Miami, tenía solo 15 años cuando se infiltró en reiteradas ocasiones en el sistema del Departamento de Defensa de Estados Unidos (DoD) y a los servidores de la Administración Nacional de Aeronáutica y del Espacio (NASA). Debido a que cometió los delitos como menor de edad, fue sentenciado a detención de menores por seis meses, al declararse culpable de dos cargos de 'delincuencia juvenil', ya que los delitos informáticos aún no estaban del todo tipificados en la ley estadounidense.

El portal de ESET, WeLiveSecurity, realizó un recopilatorio de personas que fueron condenadas por cometer delitos informáticos [10]:

David L. Smith de New Jersey, recibió una condena de 20 meses de prisión en 2002, después de que se declarara culpable de crear y propagar códigos maliciosos. Fue

el creador de Melissa, también conocido como W97M, fue uno de los virus que más daño ha causado en Internet al afectar miles de cuentas de correo electrónico y que causó más de 80 millones de dólares en daños a las empresas estadounidenses.

A 2 años y 2 meses de cárcel fue condenado Adam Botbyl en el 2004 después de que fuera encontrado culpable de sustraer los números de las tarjetas de crédito de los compradores online de la conocida cadena de almacenes Lowe luego de que logró acceder a los sistemas de la empresa conectándose a través de una red inalámbrica.

En el mismo año, Max Ray Vision, conocido por el alias iceman, es un ciberdelincuente norteamericano que fue condenado a 13 años de prisión, una de las condenas más severas que se había visto hasta esa fecha por un delito informático. En este caso, el delito también estaba relacionado con el robo de información financiera: alrededor de dos millones de tarjetas de crédito.

El 9 de mayo de 2006 Jeanson James Ancheta se declaró culpable de cuatro cargos por delitos graves por violar la Sección 1030 del Código de los Estados Unidos, Fraude y actividades relacionadas en conexión con computadoras y recibió una condena de 57 meses. James tiene el título de ser la primera persona en ser acusada y condenada por llevar a cabo ataques de denegación de servicios (DoS) utilizando cientos de computadoras zombis o botnets.

James Jeffery, de 38 años, fue condenado a 32 meses en el año 2012 por llevar a cabo un ataque al sitio web del Servicio Británico de Asesoría de Embarazos, para robar información de más de 10.000 mujeres que se habían registrado y publicó los datos de acceso de uno de los administradores del sitio.

Al mismo tiempo, Albert González, nacido en Cuba, era condenado a 20 años de cárcel, la pena más larga impuesta hasta ese momento por cometer un ciberdelito. Albert fue el responsable de uno de los fraudes más grandes de la historia. Utilizando técnicas de infiltración de código SQL, entre 2005 y 2007 logró robar alrededor de 170 millones de números de tarjetas de crédito y claves de cajeros automáticos.

Durante el año 2013 la condena de 24 meses de reclusión fue aplicada al hacker británico Lewys Martin luego de ser encontrado culpable de realizar accesos no autorizados a diversos sistemas de prestigiosas universidades inglesas, sitios de policía y gubernamentales del Reino Unido.

En diciembre de 2015, unas 230.000 personas quedaron a oscuras durante seis horas después de que piratas informáticos se infiltren en tres empresas de energía y desactivaran temporalmente los generadores en tres regiones de Ucrania. El Servicio de Seguridad de Ucrania culpó a las autoridades rusas por dicho ataque. Varias empresas privadas de seguridad estadounidenses que investigaron el evento mencionaron que podría haberse originado en Rusia. Se cree que este fue el primer ataque exitoso de piratas informáticos en una red de distribución de electricidad.

Al año siguiente, piratas informáticos filtraron miles de correos electrónicos del Comité Nacional Demócrata (DNC), la junta directiva del Partido Demócrata, durante las elecciones presidenciales de 2016. La filtración avergonzó al liderazgo del partido, quien expresó su desdén en algunos correos electrónicos por la campaña de Bernie Sanders, un candidato que había competido con Hillary Clinton para convertirse en el candidato presidencial del partido.

El Departamento de Justicia de Estados Unidos acusó más tarde a 12 rusos, que se creía que eran agentes de inteligencia militar de Rusia, por llevar a cabo el ataque cibernético [9].

Al detallar los delitos informáticos cometidos en el Ecuador podríamos mencionar los siguientes:

Según la empresa Kaspersky Lab, dedicada a la seguridad informática, estima que durante el 2010 por este tipo de delitos se han perdido cerca de 2 millones de dólares y en el año 2011 aproximadamente otros 5 millones. Así mismo, la publicación indica que en el mes de diciembre del 2011 se reportaron 1179 ataques a los sistemas de prevención de intrusos (IPS por sus siglas en inglés) [11].

La Fiscalía General del Estado ha publicado en su sitio web una infografía estadística que muestra los delitos informáticos cometidos en el país entre 2009 y 2014. Las provincias con el mayor porcentaje de incidentes son Pichincha con el 47.38 %, Guayas con el 27.57 % y en tercer lugar El Oro que registra un 5.24 %. La clonación de tarjetas y el robo de contraseñas se encuentran entre los delitos informáticos denunciados con mayor frecuencia [12].

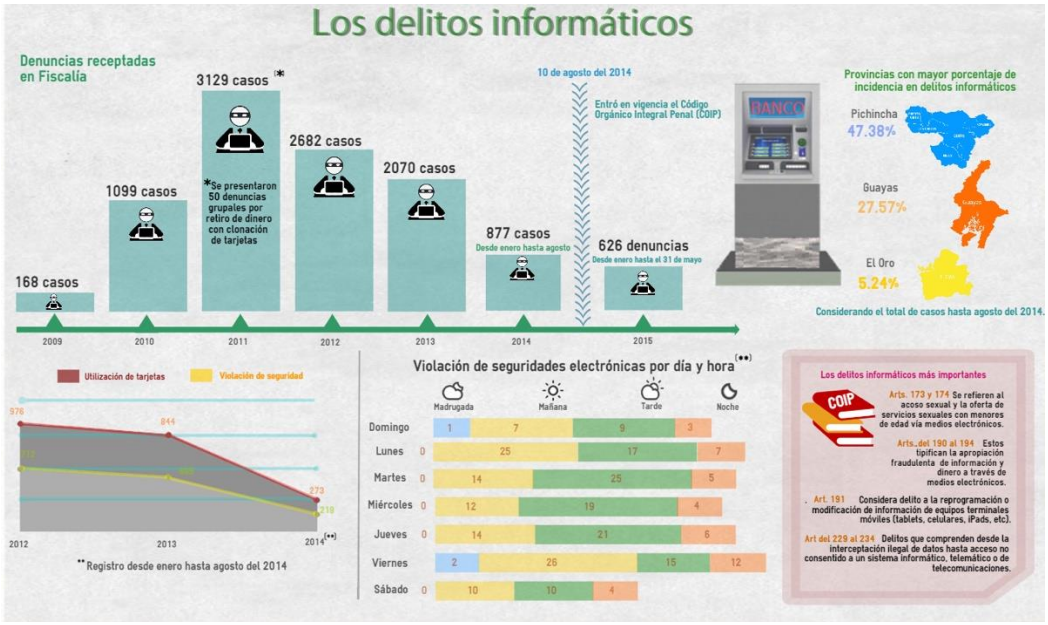

Figura 1. Estadísticas de los delitos informáticos en Ecuador, Fiscalía General del Estado, 2014

3.1.2 Ley de protección de datos

La protección de datos personales es una de las ramas del derecho más notables en el presente. Surgió como un mecanismo de protección de la privacidad en países europeos como Francia y Alemania a fines de la década de los setenta.

En mayo de 2016, el Consejo Europeo promulga el Reglamento General de Protección de Datos (RGPD) y el 25 de mayo de 2018 entró en vigor.

La regulación no sólo cambia la protección de datos personales a escala mundial, además implementa cambios profundos en materia de seguridad de la información, ya que se basa en la gestión de riesgos. Su ámbito de aplicación va más allá del territorio y todos los organismos públicos y privados con flujo de datos

automatizado deben cumplirlo. Varios estados de Estados Unidos han optado por seguir el camino trazado en la sentencia. Asimismo, varios países latinoamericanos han adoptado recientemente leyes exhaustivas sobre la privacidad/protección de datos y se encuentran en proceso de reforma para acoplarse a la normativa europea. Por ejemplo, Brasil decidió “elevar el estándar de protección de datos para cumplir con los parámetros europeos” y Chile debatía un proyecto de ley para adecuarse [13].

De la misma manera, este marco normativo incluye una serie de principios a seguir cuando se traten de datos personales: licitud, lealtad, transparencia, legitimidad, finalidad, pertinencia y minimización, así como la adecuación del tratamiento, consentimiento, confidencialidad, calidad, conservación y seguridad de estos [14].

Con la anticipación de las nuevas tecnologías y la globalización, cada momento es más tratable maltratar la privacidad de las personas y efectuar dolencia de sus datos personales. Estos cambios innovadores plantean nuevos desafíos a las leyes a encabezar los datos personales. Por esta razón, es muy importante describir el derecho a la protección de datos como un derecho separado, aunque muy pocos países han logrado darle tal tratamiento a este derecho.

Para comprender el insuficiente progreso, se observa que existen 193 países oficialmente reconocidos por la ONU, pero solo 120 de ellos han promulgado leyes relacionadas con la salvaguarda de datos. Esto representa el 61 % de los países. Sin embargo, la mayoría de ellos carece de un nivel elevado de protección de datos o de legislación especializada que lo regule [15].

Vale recordar que, el dato personal no es necesariamente un dato íntimo, pero cualquier información sobre una persona es suficiente, ya que la privacidad es independiente y no determina la calidad de los datos personales. Por lo tanto, una dirección de correo electrónico, un número de teléfono o la dirección IP podrían considerarse datos de carácter personal.

3.1.3 Ley Orgánica de Protección de Datos Personales de Ecuador

Debemos basarnos en el hecho de que las normas jurídicas deben ser coherentes con la realidad social. ¿Cuál es el contexto en Ecuador donde la sociedad no necesite la creación de estándares y una ley de protección de datos? La competencia podría ser repartida entre: el Estado, las empresas y los ciudadanos sin necesidad de promulgar leyes que restrinjan y regulen este derecho. Además de la escasez de un marco legal, existe poca doctrina o jurisprudencia en el país sobre este tema.

Muchos han sido los intentos en Ecuador de regular el derecho a la protección de datos personales mediante una ley destinada a este fin. Como parte de la acción estratégica del Eje 6 del Plan Nacional de la Sociedad de la Información y el Conocimiento 2018 - 2021, se anunció un proyecto de ley en materia de protección de datos personales. El 19 de septiembre de 2019, Lenín Moreno, presidente del Ecuador, presentó al poder legislativo el Proyecto de Ley Orgánica de Protección de Datos Personales. El principal propósito del proyecto era "regular y proteger el ejercicio del derecho a la protección de datos personales."

Más allá de las intenciones del Plan Nacional, la precisión de una ley normativa surge de una serie de situaciones preocupantes. En septiembre de 2019, ZDNet comunicó que existió una filtración masiva de datos personales, entre los que se encontraba información sensible de ciudadanos ecuatorianos [5].

Este no es un caso ocasional. En el Ecuador, la privacidad se viola todos los días. Por citar un ejemplo, en plataformas como Mercado Libre o tiendas físicas se comercializan bases de datos actualizadas de organismos gubernamentales como la Dirección General de Registro Civil, Identificación y Cedulación o el Consejo Nacional Electoral. El almacenamiento y venta de dichos datos está prohibida. Se vuelve urgente que exista un marco jurídico que mantenga un estándar de protección de datos personales que reglamente completamente el consentimiento del titular y la finalidad con la que se procesan sus datos [15].

El pleno de la Asamblea Nacional de Ecuador, con 118 votos a favor, el 10 de mayo de 2021 aprobó su propia Ley Orgánica de Protección de Datos con varios incisos similares al reglamento de la Unión Europea.

El poder judicial se ha sometido a un extenso proceso de desarrollo participativo, que comenzó en octubre de 2017. El proceso se ha llevado a cabo en colaboración con una variedad de disciplinas, incluidos expertos, y los sectores público y privado en la materia. En este contexto, se han organizado una serie de mesas de trabajo con organismos del sector de las telecomunicaciones, como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y la Agencia de Regulación y Control Postal (ARCPostal), Correos del Ecuador EP, Corporación Nacional de Telecomunicaciones (CNT), Registro Civil y Ministerio de Comunicaciones y Sociedad de la Información, Mintel. Con carácter de ley técnica, regula la creación de una autoridad de control en materia de protección de datos, que será la encargada de comprobar que se han cumplido las obligaciones previstas en la norma para el buen uso de los datos [16].

3.1.4 Ley de Protección de Datos Personales y Acción de "Habeas Data" de Uruguay

El "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" fue aprobado por la Ley 19.030 y contenía principios básicos en materia de protección de datos.

Como se exponen los motivos del Poder Ejecutivo, "Con la entrada en vigencia de la mencionada Ley el 1 de enero de 2013, Uruguay se convirtió en el primer país no europeo en ser parte del Convenio y su Protocolo Adicional. (…)" Hoy en día Uruguay cuenta con la Ley 18.331 (la "LPDP"), la cual sufrió una modificación mediante la Ley 19.670, con la finalidad de actualizarla y adecuarla, a los estándares europeos.

A principios de 2020 se publicó el Decreto 64/2020 (publicado en el Boletín Oficial del 21 de febrero de 2020), por el que se reglamentan los artículos 37 a 40 de la Ley 19.670. Este Reglamento requiere que las personas que tratan datos personales

consideren la naturaleza de los datos que manejan, el tratamiento que realizan, los riesgos asociados y las implicaciones de su realización, y los procesos y medios establecidos para dar cumplimiento a la LPDP. Esta conlleva procedimientos y políticas documentadas para la protección de datos personales, cuyo contenido se especifica en la norma ("la documentación de las medidas incluirá, al menos, las formas, medios, fines y procedimientos para su cumplimiento: normativa de protección de datos, planes de mecanismos para responder a las brechas de seguridad y el papel del oficial de protección de datos cuando corresponda.") [17].

El 30 de junio de 2020 el Poder Ejecutivo de Uruguay presentó al Poder Legislativo un nuevo proyecto de ley, cuyo objeto es ratificar el Protocolo Modificatorio del Acuerdo para la Protección de las Personas Interesadas en el Tratamiento de Datos Personales ("Acuerdo Original") . Este protocolo se firmó el 10 de octubre de 2018 [18]. Es una norma destinada a actualizar los términos del documento original, hacer frente a las nuevas realidades y fortalecer la protección de los datos personales. Asimismo, se ha certificado el cumplimiento por parte de Uruguay del modelo de protección de datos personales desarrollado por los países europeos.

3.2 Definiciones

En esta sección mencionaremos algunas definiciones necesarias para la comprensión del presente trabajo.

3.2.1 Sistema de Gestión de Seguridad de la Información

Information Security Management System – ISMS en inglés, es un conjunto de políticas y procesos de gestión y administración de los activos de información en una organización.

Su objetivo principal es ofrecer un manejo efectivo de la información garantizando los principios de confidencialidad, integridad, disponibilidad, autenticidad y no repudio [18] dejando de lado el formato o medio de almacenamiento de esta.

3.2.2 Ley orgánica

La enciclopedia online Concepto [19] describe una ley orgánica como aquella que se encarga, desde un enfoque constitucional, de la regulación de ciertas materias esenciales para el ejercicio de la democracia de un estado, como son: normas constitucionales fundamentales, libertades públicas o la articulación de los poderes de una nación.

La aprobación de un proyecto de ley orgánica requiere de un consenso y procedimiento aprobatorio por parte del poder legislativo, el cual es precedido generalmente por el parlamento, asamblea nacional o congreso de una Nación.

El precedente jurídico de una ley orgánica se encuentra en el derecho francés, concretamente en la Constitución de 1958, sobre la cual se estableció la Quinta República de Francia.

3.2.3 Dato personal

La Ley Orgánica de Protección de Datos Personales de Ecuador [20] define como datos personales a “aquel que identifica o hace identificable a una persona natural, directo o indirectamente”.

Por el contrario, la Ley de Protección de Datos Personales de Uruguay [21] establece como dato personal a “la Información de cualquier clase o tipo y que sea referida a personas físicas o jurídicas determinadas o determinables”.

3.2.4 Dato sensible

Conforme con la ley ecuatoriana [20] son “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".

Por otra parte, el reglamento uruguayo [21] determina que los datos sensibles son aquellos "datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical en informaciones referentes a la salud o vida sexual".

3.2.5 Hacker

El término hacker puede aludir a una persona experta con conocimiento en TI y que se dedica a descubrir vulnerabilidades en los sistemas informáticos; es decir, se inmiscuye detalladamente en los sistemas operativos, programación, arquitectura informática, sistemas de comunicación, entre otros.

Autores como Sweigart [22] lo definen como "un individuo que estudia un sistema informático para comprenderlo a profundidad, que pueda ser capaz de modificarlo de distintas formas, en su mayoría creativas". Por su parte, Erickson [23] señala que "un hacker resuelve problemas en maneras inimaginables comparado con aquellos que se circunscriben en resolverlos con métodos tradicionales". Incluso Palmer [24] describe el término hacker como "aquella persona que programa de manera entusiasta y aprende a detalle los sistemas de cómputo".

3.2.6 Hacking ético

El hacking ético es un conjunto de principios morales en los que un grupo de individuos deciden empezar a realizar ataques a equipos, emulando los peores escenarios, con el afán de descubrir fallos en la seguridad implementada de una empresa, organización y/o entidad. Una vez descubiertas estas vulnerabilidades o falencias, los hackers éticos generan un reporte y lo presentan al área pertinente para que se lleve a cabo una gestión de riesgos sobre los hallazgos encontrados. Bajo ningún concepto deben tratar de aprovecharse de esa vulnerabilidad [25] [26].

3.3 Estado del arte

González J., Bermeo J. y Villacreses (2018)

En su investigación hablan acerca de los "delitos informáticos en Latinoamérica en la sociedad contemporánea que ha adoptado a la informática como base para gestionar sus actividades en el mundo, como conclusión de su trabajo indican que, en la mayoría de los países estudiados, aún persisten en algunos casos los vacíos legales con respecto a la regulación del uso de la información a partir de los diferentes medios de comunicación. A pesar de que han sido múltiples los esfuerzos de los gobiernos en la lucha contra este tipo de delitos, donde se incluye la piratería, difusión de pornografía infantil, así como el uso inadecuado de la información con diferentes fines; lamentablemente aún persisten este tipo de prácticas. Los delitos informáticos no se pueden erradicar de un día para otro, pero si es posible y urgente legislar y aplicar la ley para el combate a estos delitos con más rigor, pues, aunque las autoridades competentes pongan a disposición de un Ministerio Público a estas bandas delictivas o actores individuales, lamentablemente no se tienen elementos suficientes para atribuir responsabilidades por la falta de claridad en las leyes. Las medidas a tomar en el Ecuador deben ser claras, en primera instancia capacitar a la ciudadanía sobre la realidad de estos delitos, implementar reformas a su código penal para actuar libremente mediante la aplicación de leyes dinámicas que se actualicen según se detecten el modo de operar de los responsables, además mejorar los sistemas de seguridad a nivel nacional en todos los entornos virtuales, no solo en bancos sino en sitios gubernamentales y aplicar códigos para regular el uso de las redes sociales al ejecutar dichos actos vandálicos."

Hamilton Villón, Marlon Sojos, Carlos Mendoza, Teresa Guarda y Arturo Clery (2018)

En su trabajo investigaron sobre Pharming y Phishing: delitos informáticos penalizados por la legislación ecuatoriana, mecanismos que son usados por los delincuentes informáticos que usan la ingenuidad de las personas para sustraer su información personal y captarlos para un mal uso posterior. Concluyen que no

existe una legislación penal adecuada, lo que provoca que cada vez más delitos parecidos queden en la impunidad. Por esta razón es necesaria la toma de medidas preventivas propias que eviten que este tipo de delitos se incrementen. Como, por ejemplo, no dar indiscriminadamente datos personales, pues se desconoce con exactitud, en donde se almacenan y quien va a hacer uso de ellos. Ser víctima de estos delitos, es prácticamente una decisión propia y del uso responsable que se le da a la información personal.

María Fernanda González Hernández (2019)

Gonzáles en su monografía acerca de la Ciberseguridad en Uruguay "realiza un análisis de la situación general en materia a nivel regional, para luego profundizar en el estudio de la Estrategia Interamericana de Seguridad Cibernética de la OEA y el alcance o influencia que ha tenido ésta en Uruguay. Luego de haber realizado una descripción en profundidad de la Estrategia en Ciberseguridad de la OEA y las pautas o recomendaciones que fijan cada uno de los organismos que la protagonizan, se realizó el análisis de la influencia de estos sobre Uruguay. A partir de este trabajo, se puede afirmar que Uruguay cumple en mayor o menor medida con las recomendaciones del CICTE (Comité Interamericano contra el Terrorismo), la CITEL (Comisión Interamericana de Telecomunicaciones) y las REMJA (Reuniones de Ministros de Justicia u otros Ministros, Fiscales y Procuradores Generales de las Américas), más específicamente del Grupo de Trabajo en Delito Cibernético. En cuanto a lo que propone el CICTE, Uruguay cumple con la mayor parte de las condiciones para integrar la Red Interamericana de Vigilancia y Alerta. Cuenta con su propio D-CSIRT (CERTuy), que reúne los requisitos exigidos. A nivel regional, coopera en ciberseguridad, y cuenta además con el SOC como organismo que realiza esfuerzos en el mismo sentido. Lo que propone la CITEL no se ve reflejado de manera tan clara en el panorama nacional. Uruguay no cuenta con normas técnicas en ciberseguridad, y no tiene una participación importante en los cursos brindados por el organismo en la materia. Aun así, participa activamente y organiza foros para el intercambio de información con otros Estados, y también entre el sector público y privado."

Narda J. Ortiz Campos (2019)

La autora en su revisión bibliográfica señala que “el avance tecnológico y la creciente accesibilidad a Internet que tienen las personas en el mundo ha sido de utilidad para la masificación en la creación y utilización de diferentes sitios web y aplicaciones. No obstante, esos beneficios se tornan peligrosos cuando se infiltran entre los servicios del Internet programas maliciosos que de forma silenciosa pueden dañar no sólo los equipos tecnológicos sino también las finanzas de las personas, empresas y gobiernos”. Se detallan problemas existentes en la lucha contra los delitos informáticos como: Incertidumbre del alcance del delito cometido lo que dificulta cuantificar los daños causados y la determinación de condenas. En segundo lugar, la dimensión transnacional dificulta realizar las investigaciones correspondientes dado que los delitos se pueden cometer en un país y las víctimas pueden estar en otro, lo que se contrapone con el principio de territorialidad. Finalmente, los enfoques jurídicos de cada país aún no son compatibles lo que provoca que no exista una cooperación internacional eficaz en la lucha contra el ciberdelincuente.

Felipe Nicolás Roldán Carrillo (2020)

Menciona que “los datos personales son el nuevo petróleo del internet y la nueva moneda de la economía digital. Este avance desenfrenado de la tecnología puede acarrear ciertas vulneraciones.

La protección de datos personales atraviesa una metamorfosis normativa a nivel mundial. Son dos modelos de protección por los que se puede optar al momento de incorporar estos cambios legislativos: europeo y estadounidense. En el modelo europeo la protección de datos personales se encuentra debidamente regulada. Existe una autoridad de inspección y de sanción. En cambio, en el modelo estadounidense la autorregulación o regulación mínima es el principal componente. No hay una autoridad estatal que se encargue de velar por este derecho fundamental. Los titulares deberán acudir a la instancia judicial para determinar la responsabilidad de la empresa por su actuar y solicitar una indemnización.”

Mario Ramiro Aguilar Martínez, Diego Patricio Gordillo Cevallos, Julio Alfredo Paredes López y Gabriela Paulina León Burgos (2022)

Este artículo aborda “la protección a los datos personales debido a la presión mediática generada a partir de la publicación de la empresa vpnMentor sobre la sustracción ilegal de datos personales almacenada en servidores de Novastrat.” En consecuencia, permitió la publicación en el Registro Oficial de la Ley Orgánica de Protección de Datos. Se concluye que “a pesar de contar con una Ley de Protección de Datos Personales, los datos de los ecuatorianos no se encuentran garantizados y para que esto se produzca se requiere un cambio no solo de la parte jurídica, sino más bien de la sociedad.”

4 Reseña histórica de las Leyes de Protección de Datos Personales de Ecuador y Uruguay

Tanto Ecuador como Uruguay han adoptado leyes de protección de datos personales para salvaguardar la privacidad y los derechos de los individuos en el entorno digital. Estas leyes establecen principios, derechos y obligaciones para el tratamiento de los datos personales, buscando asegurar un adecuado nivel de protección y promover la confianza en el uso de la información personal.

Las leyes sobre la protección de datos se basan en la privacidad de las personas. Sin embargo, el significado de privacidad y el origen del derecho a la privacidad de un individuo pueden ser diferentes. Por esta razón, las leyes y normas que rigen este derecho varían de un país a otro [27].

Bajo este contexto, el 10 de mayo de 2021 Ecuador aprobó su Ley Orgánica de Protección de Datos, con varias disposiciones similares al Reglamento General de Protección de Datos (RGPD). Si bien es cierto se tiene un tiempo de transición de dos años para la aplicación de la ley, una vez que se dispuso su publicación el 22 de mayo de 2021 en el Registro Oficial, las instituciones públicas y privadas deben iniciar su preparación para el cumplimiento, entendiendo que no es sólo un asunto jurídico, sino sobre todo de gestión. Para proteger los derechos y libertades la protección de datos se basa en la gestión de riesgos. Esto ha cambiado significativamente los procesos relacionados con la seguridad de la información [28].

En cambio en Uruguay cuenta con el estatus de país adecuado en los términos de la Comisión Europea, por Decisión 2012/484/EU, del 21 de agosto de 2012. De tal

manera, se concluiría que Uruguay es una de las naciones de Sudamérica con la mayor regulación en materia de protección de datos personales.

El objetivo de una ley de protección de datos personales, como ya lo hemos indicado, es establecer lineamientos para las actividades relacionadas con la recopilación y el procesamiento de datos por parte de entidades públicas y privadas como también evitar la injerencia arbitraria en el normal desarrollo de la vida de los ciudadanos, independientemente del lugar donde se produzca dicha injerencia.

En la actualidad, en todas las interacciones sociales, tanto con entes públicos como con las organizaciones privadas, se transfieren datos personales o cualquier información relativa a una persona identificada o identificable, que operan en todos los campos de la economía, las actividades sociales y la cultura. Sin embargo, debido a la misma frecuencia y cotidianidad con la que se comparte información personal, muchas veces perdemos de vista que es la puerta de entrada a nuestra vida y una oportunidad para socializar. Una regulación de privacidad nos permite, como ciudadanos, contar con herramientas especiales para restringir el uso de la información [29].

5 Delitos tipificados en las Leyes de Protección de Datos Personales de Ecuador y Uruguay

5.1 Ecuador

El desarrollo de las tecnologías de la información y su proliferación mediante servicios y aplicaciones de Internet, como la mensajería instantánea, las redes sociales o el correo electrónico en dispositivos inteligentes, propicia el uso de la información para la realización de actividades tipificadas como delitos. Palabras como "ciberacoso, ciberbullying, sexting, grooming, phising, pharming o carding", son términos en inglés que se refieren a situación de acoso, intimidación, coacción, divulgación, agresión sexual, violencia de género o incluso estafa y cada vez son más familiares para nosotros [30].

En la LOPDP ecuatoriana no tipifica delitos, pero podemos revisar algunos artículos que hacen referencia algunas infracciones y sanciones de los ciberdelitos [31]:

En el "Artículo 67 de infracciones leves del responsable de protección de datos nos indica. Se consideran infracciones leves las siguientes:

- No tramitar, tramitar fuera de término previsto o negar injustificadamente la peticiones o quejas realizadas por el titular.
- No implementar protección de datos desde el diseño y por defecto.
- No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales.
- Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales.

- Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales."

En el "Artículo 68 de infracciones graves del responsable de protección de datos. Se consideran infracciones graves las siguientes:

- No implementar medidas administrativas, técnicas y físicas: organizativas y jurídicas, a fin de garantizar el tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.
- Utilizar información o datos para fines distintos a los declarados.
- Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.
- No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales las particularidades del tratamiento y de las partes Involucradas.
- No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarla.
- No implementar medidas técnicas organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de datos personales que hayan sido identificadas.
- No notificar a la Autoridad de Protección de Datos Personales y al titular, de vulneraciones a la seguridad y protección de datos personales, cuando afecte los derechos fundamentales y libertades individuales de los titulares.
- No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos fundamentales y libertades individuales de los titulares.

- No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales.
- No mantener actualizado el Registro Nacional de Protección de datos personales de conformidad a lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones, emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.
- No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente ley y su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.
- No designar al delegado de protección de datos personales cuando corresponde.
- No permitir y no contribuir a la realización de auditorías o inspecciones por parte del auditor acreditado por la Autoridad de Protección de Datos Personales.
- Incumplir las medidas correctivas o cumplir de forma tardía, parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve, o incurre de forma reiterada en faltas leves."

En el "Artículo 69 de infracciones leves del encargado de protección de datos. Se consideran infracciones leves las siguientes:

- No colaborar con el responsable del tratamiento de datos personales, para que este cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales.
- No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimento de las obligaciones establecidas en la presente ley, su reglamento, directrices, lineamientos y

regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

- No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por la Autoridad de Protección de Datos Personales.
- Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales."

En el "Artículo 70 de infracciones graves del encargado de protección de datos. Se consideran infracciones graves las siguientes:

- Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente Ley y su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.
- No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional.
- No suscribir contratos que contengan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el personal a cargo del tratamiento de datos personales o quien tenga conocimiento de los datos personales.
- No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales.
- No implementar medidas preventivas y correctivas en la seguridad de los datos personales a fin de evitar vulneraciones.
- No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales, una vez haya culminado su encargo.
- Proceder a la comunicación de datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.

- Incumplir las medidas correctivas o cumplirlas de forma tardía, parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.
- No notificar al responsable del tratamiento de datos personales sobre cualquier vulneración de la seguridad de datos personales conforme dispone esta ley o hacerlo con retraso injustificado."

En el "Artículo 71 sanciones por infracciones leves:

La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:

- Servidores o funcionarios del sector público por cuya acción o emisión hayan incurrido en alguna de las infracciones leves establecidas en la presente ley, serán sancionados con una multa de uno a diez salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.
- Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0,1 % y el 0,7 % calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa."

En el "Artículo 72 de sanciones por infracciones graves:

La Autoridad de Protección de Datos Personales impondrán las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción grave, conforme a los presupuestos establecidos en el presente Capítulo:

- Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionados con una multa de entre 10 a 20 salarios

básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.

- Si el responsable encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0,7 % y el 1 % calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad."

5.2 URUGUAY

Durante los últimos 10 años, Uruguay se ha destacado por sus logros en el campo de las tecnologías de la información y la comunicación (TIC). Sin embargo, hay una categoría de medición en la que la república uruguaya aun no sobresale: la clasificación e investigación de ciberdelitos.

En Uruguay, varios proyectos de ley para tipificar los delitos informáticos han sido presentados al Poder Legislativo por iniciativa de diferentes partidos políticos. Algunas de estas propuestas son más extensas que otras, aunque ninguna ha pasado más allá del debate en el Congreso.

En la actualidad, Uruguay no cuenta con una ley específica de delitos informáticos; sin embargo, esto no quiere decir que algunos delitos que son considerados como informáticos no existan en su ordenamiento jurídico, tanto por doctrina como por estándares y reglamentos internacionales relacionados a la materia. Por dar algunos ejemplos se presentan los siguientes cuerpos legales vigentes en Uruguay:

La Ley 17.616 que modificó la Ley de Derechos de Autor de 1937 introduce a los bienes protegidos a los programas de computadora y las bases de datos. Su Artículo 46 establece una serie de actos que pueden ser castigados penalmente por infringir

en contra de la protección de derechos de autor, cuando se realicen “por cualquier medio”.

La Ley 17.815 sobre Violencia Sexual contra Niños, Niñas, Adolescentes o Personas con Discapacidad tipifica como delito la fabricación, producción, venta, distribución y facilitación, por cualquier medio, de material pornográfico con menores o personas con algún tipo de discapacidad.

La Ley 18.383 de 2008 que modifica el Artículo 217 del Código Penal tipificó el delito de atentado contra las telecomunicaciones alámbricas e inalámbricas, sancionado con pena privativa de libertad desde tres meses a tres años.

El Artículo 4 de la Ley 18.600 de Documento y Firma Electrónica dispone que: “El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del Código Penal, según corresponda.” Es decir, para que los jueces no utilicen analogías in malam partem, el legislador prefirió equiparar los documentos electrónicos con los documentos en papel y así trasladó el capítulo del Código Penal sobre Falsificación Documentaria a los nuevos medios.

Desde la adopción del Convenio de Budapest a nivel internacional, Uruguay había propuesto tres proyectos legislativos al respecto. Fue expuesto por primera vez por el senador Tabaré Viera en el 2010 y tenía como objetivo introducir los delitos enumerados en el Convenio y que aún no se encontraban en el ordenamiento jurídico uruguayo. Posteriormente, en el 2014 AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento), a través del Poder Ejecutivo, presentó su propia propuesta, la cual también terminó archivada. Finalmente, en mayo de 2016 se presentó a estudio de la Comisión de Innovación, Ciencia y Tecnología un nuevo proyecto, presentado nuevamente por el senador Viera con una redacción diferente a la presentada en 2010. Estas tres propuestas se sumaron a las iniciativas que presentó el senador Pedro Bordaberry en marzo 2015 para agregar al Código Penal los delitos de: difusión no consentida de imágenes privadas o “pornografía de venganza”, suplantación de identidad y ciberacoso hacia

menores de edad. Como demuestran los múltiples intentos de propuestas legislativas presentadas, la tipificación de delitos mediante el uso de computadores está latente en el sistema de política uruguayo.

A partir de 2012, una división especializada en delitos informáticos ha estado activa en el Ministerio del Interior. Esta oficina es responsable de investigar dónde se ha utilizado la tecnología como medio delictivo. Además de la Oficina de Delitos Tecnológicos, también existen dos centros de respuesta a incidentes informáticos: CERTuy y D-CSIRT.

El Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) fue creado a través del Artículo 73 de La Ley de Rendición de Cuentas del Ejercicio 2007 (Ley 18.362) y dentro de las atribuciones de AGESIC. Algunas de sus funciones son:

- Difusión de buenas prácticas en la materia.
- Concentrar, coordinar la reacción a incidentes informáticos e implementar acciones preventivas adecuadas.
- Sugerir y asesorar en el diseño de procedimientos, políticas, métodos y buenas prácticas en materia de seguridad de la información a la función pública.
- Proporcionar soporte en la etapa de implementación de estas políticas.

Por otro lado, el Ministerio de Defensa también dispone de su propio centro de respuestas, llamado D-CSIRT. Fue creado igualmente bajo el mismo artículo y reglamentado por el Decreto 36/2015. Es el responsable de la coordinación de las actividades relacionadas con los incidentes de seguridad de la información de la cartera de estado.

Las tres agencias (Delitos Tecnológicos, CERTuy y D-CSIRT) son parte de organizaciones regionales e internacionales para el intercambio de información. Trabajan juntas en colaboración, de forma coordinada, a pesar de que no existe un espacio formal para la cooperación. Se están haciendo esfuerzos para formalizar los protocolos y se mejoren los intercambios de información.

La información estadística es un activo importante en el campo de los delitos informáticos para saber qué acciones son socialmente condenadas y ameritan ser sancionadas penalmente. El Observatorio Nacional sobre Violencia y Criminalidad en sus informes anuales no excluyen datos sobre delitos informáticos o que tengan un elemento tecnológico en su ejecución. Por su parte, CERTuy desde 2014, difunde año a año, estadísticas que muestran las maniobras técnicas más utilizadas en los incidentes de seguridad reportados.

La Ley 18.331, que establece el sistema de protección de datos personales y el proceso de habeas data en el ordenamiento jurídico, excluye a los imputados por mal manejo de datos personales. La pena más severa prevista en la Ley es la clausura de las bases de datos, que la Oficina Reguladora y de Control de Datos Personales ha aplicado una única ocasión en casi once años, desde su creación. Cualquier modificación al sistema existente deberá respetar los anteriores derechos, garantías y obligaciones, para que su interpretación sea coherente y consistente.

A continuación, se transcribe el Artículo 35 sobre las sanciones descritas en la Ley 18.331 [21]:

“Artículo 35 (Potestades sancionatorias). - El órgano de control podrá aplicar las siguientes sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en caso que se violen las normas de la presente ley, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida:

- Observación.
- Apercibimiento.
- Multa de hasta 500.000 UI (quinientas mil unidades indexadas).
- Suspensión de la base de datos respectiva por el plazo de cinco días.
- Clausura de la base de datos respectiva. A tal efecto se faculta a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento a promover ante los órganos

jurisdiccionales competentes la clausura de las bases de datos que se comprobare que infringieren o transgredieren la presente ley.

Los hechos constitutivos de la infracción serán documentados de acuerdo a las formalidades legales. La clausura deberá decretarse dentro de los tres días siguientes a aquél en que la hubiere solicitado la Unidad Reguladora y Control de Datos Personales, la cual quedará habilitada a disponerla por sí en caso que el Juez no se pronunciare dentro de dicho término.

En este último caso, si el Juez denegare posteriormente la clausura, ésta deberá levantarse de inmediato por la Unidad Reguladora y Control de Datos Personales.

Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la clausura, no tendrán efecto suspensivo.

Para hacer cumplir dicha resolución, la Unidad Reguladora y Control de Datos Personales podrá requerir el auxilio de la fuerza pública. La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura Ley 15.750, de 24 de junio de 1985, sus modificativas y concordantes.

Las resoluciones firmes de la Unidad Reguladora y Control de Datos Personales que impongan sanciones pecuniarias constituyen título ejecutivo a sus efectos."

El 3 de agosto de 2021 el legislador Sebastián Cal presentó en la Asamblea de Uruguay un nuevo proyecto de ley que pretendía tipificar y regular los delitos informáticos o ciberdelitos. En dicho proyecto se planteó crear nueve delitos y una campaña nacional de educación sobre ciberdelincuencia y sus delitos [32].

Además, se trabajaba en una modificación a la Ley 18.331, donde las empresas, públicas o privadas, que gestionan una determinada cantidad de datos de personas, tengan que mantener un nivel mínimo de seguridad. Esta propuesta aún no fue presentada y Cal esperará a que se apruebe el proyecto sobre ciberdelitos para continuar con su presentación [33].

A continuación, se desarrolla un análisis a cada delito propuesto en el proyecto de ley [32]:

- Stalking u hostigamiento: La divulgación de fotos íntimas, uno de los hechos punibles del proyecto, estaba previsto en la Ley 19.580 del 22 de diciembre de 2017 y cuyo texto se detalla a continuación: "Artículo 92 (Divulgación de imágenes o grabaciones con contenido íntimo).- El que difunda, revele exhiba o ceda a terceros imágenes o grabaciones de una persona con contenido íntimo o sexual, sin su autorización, será castigado con una pena de seis meses de prisión a dos años de penitenciaría. En ningún caso se considerará válida la autorización otorgada por una persona menor de dieciocho años de edad. Este delito se configura aun cuando el que difunda las imágenes o grabaciones haya participado en ellas. Los administradores de sitios de internet, portales, buscadores o similares que, notificados de la falta de autorización, no den de baja las imágenes de manera inmediata, serán sancionados con la misma pena prevista en este Artículo."
- Grooming: En Uruguay está tipificado a través de la Ley 19.580 y se reproduce a continuación: "Artículo 277-BIS.- El que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de trasmisión de datos, contactare a una persona menor de edad o ejerza influencia sobre el mismo, con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico u obligarlo a hacer o no hacer algo en contra de su voluntad será castigado con pena de seis meses a cuatro años de penitenciaría."
- Estafa informática: Deja pendiente el problema de la inducción a error a un sistema informático y únicamente castigaría las inducciones a error por parte de un individuo (si bien se describe la manipulación informática o artificios afines, no es explícito si engañar a un sistema informático es punible).
- Daños informáticos: El proyecto se alinea a lo propuesto por Budapest (que sugiere llamarlo atentados contra la integridad de los datos) pero no

justifica, desde un punto de vista punitivo, el por qué propone pena de reclusión.

- Acceso ilícito a datos informáticos: El proyecto se alinea con el Convenio de Budapest (la propuesta es designarlo como acceso Ilícito), pero en materia penal no se justifica por qué se plantea una sanción de privación de libertad para el caso del acceso informático cuando la figura del Artículo 297 del Código Penal (interceptación de noticia telegráfica) preveía únicamente una pena pecuniaria.
- Vulneración de datos: Es posible una derogación tácita del Artículo 300 del Código Penal cuya redacción se transcribe: "Artículo 300 (Conocimiento fraudulento de documentos secretos).- El que, por medios fraudulentos, se enterare del contenido de documentos públicos o privados, que por su propia naturaleza debieran permanecer secretos, y que no constituyeran correspondencia, será castigado siempre que del hecho resultaren perjuicios, con 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables) de multa." Otra situación se presenta con el Artículo 11 de la Ley 18.331.- "Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros. Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (Artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular."
- Robo de identidad: No está tipificado en Uruguay ni mencionado en Budapest. La legislación norteamericana podría ser una posible referencia, ya que la reforma de 2008 de la “Computer Fraud and Abuse Act” a través

de la “Identity Theft Enforcement and Restitution Act”, reguló la suplantación de identidad como un delito.

- Terrorismo digital: Aunque el Convenio de Budapest no incluye esta propuesta de clasificación, la redacción coincide parcialmente con la redacción del estándar estadounidense de 2001, USA PATRIOT (en inglés “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”) Act. Efectivamente esta norma delimita la definición de terrorismo electrónico o ciberterrorismo a los actos de sabotaje y espionaje al igual que esta propuesta. La Patriot Act define el delito informático como un acto de terrorismo, aunque no incluye todos los delitos enumerados en la “Computer Fraud and Abuse Act” (CFAA), lo cual muestra afán por ajustar la definición de terrorismo cibernético a los hechos de sabotaje y espionaje.
- Abuso de dispositivos: Esto es consistente con lo que se plantea en Budapest (la propuesta lo llama abuso de equipos e instrumentos técnicos) pero desde el punto de vista punitivo, la pena de reclusión no es justificable.

6 Análisis Comparativo

Tanto Uruguay como Ecuador cuentan con leyes de protección de datos personales que establecen reglas y principios para garantizar la privacidad y seguridad de la información personal de sus ciudadanos.

A continuación, presentamos las similitudes entre la Ley de Protección de Datos Personales de Uruguay y la Ley Orgánica de Protección de Datos Personales de Ecuador.

Ecuador:

La Ley de Protección de Datos Personales de Ecuador tiene como principal propósito resguardar los datos personales de los ciudadanos ecuatorianos y fue aprobada en 2018.

Principios fundamentales: La LOPDP establece los principios fundamentales para el tratamiento de datos personales como: el consentimiento, la finalidad legítima, la proporcionalidad, la calidad de los datos y la seguridad de la información.

Derechos del titular de los datos: La ley reconoce los derechos del titular de los datos como: el acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales.

Transferencia internacional de datos: La LOPDP regula la transferencia internacional de datos personales y establece que los datos solo pueden ser transferidos a países que proporcionen un nivel adecuado de protección de datos o mediante garantías apropiadas.

En Ecuador se nombrará un ente regulador encargado de que las organizaciones cumplan a cabalidad con la LOPDP.

Uruguay:

Ley de Protección de Datos Personales y Acción de "Habeas Data": En Uruguay, la ley de protección de datos personales es la Ley N° 18.331 fue promulgada en 2008 y regula también la acción de "habeas data".

Principios fundamentales: La ley establece principios fundamentales similares a los de Ecuador como: el consentimiento, la finalidad, la proporcionalidad, la calidad y la seguridad de los datos.

Derechos del titular de los datos: La normativa uruguaya reconoce los derechos del titular de los datos, incluyendo el acceso, la rectificación, la cancelación y la oposición al tratamiento de sus datos personales.

Transferencia internacional de datos: La ley uruguaya permite la transferencia de datos personales a países que brinden un nivel adecuado de protección de datos o mediante garantías apropiadas.

Autoridad de control: La Unidad Reguladora y de Control de Datos Personales es la entidad encargada de supervisar y hacer cumplir la ley de protección de datos en Uruguay.

A pesar de estas similitudes que hemos evidenciado, también hay diferencias importantes entre las leyes de protección de datos personales de Ecuador y Uruguay. Estas diferencias pueden incluir aspectos relacionados con el ámbito de aplicación de la ley, plazos por incumplimiento y las sanciones.

Ámbito de aplicación: En términos de su ámbito de aplicación, la ley uruguaya se aplica tanto a personas físicas como jurídicas, mientras que la ley ecuatoriana se enfoca principalmente en la protección de datos de personas naturales.

Transferencia internacional de datos: En Uruguay, se requiere una autorización previa de la Unidad Reguladora y de Control de Datos Personales para realizar transferencias internacionales de datos a países que no brinden un nivel adecuado de protección. En Ecuador, la ley establece que se pueden realizar transferencias

internacionales de datos siempre que se cumplan ciertos requisitos y se garantice un nivel adecuado de protección.

Sanciones y multas: Las leyes de ambos países contemplan sanciones y multas por incumplimiento de las disposiciones de protección de datos. Sin embargo, los montos y criterios de aplicación pueden variar. En Uruguay, las multas pueden alcanzar hasta el 2 % de la facturación anual del infractor, mientras que en Ecuador las multas pueden ser de hasta 20 salarios básicos unificados.

Plazos de notificación de incidentes: En Uruguay, los responsables del tratamiento de datos deben notificar a la Unidad Reguladora y de Control de Datos Personales los incidentes de seguridad que puedan afectar los derechos de los titulares de datos en un plazo de 72 horas. En Ecuador, el responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco días después de que haya tenido constancia de ella.

La ley uruguaya, al tener más tiempo en vigencia, puede ser mucho más “madura” que la ley ecuatoriana, en esta comparación se lo evidencia; sin embargo, los autores de este trabajo consideran que el hecho de que Ecuador haya decidido impulsar esta ley representa un gran paso, ya que es de suma importancia que el Estado cuente con este instrumento. Esta ley desempeñará un papel fundamental en la defensa de la privacidad de los ciudadanos y en el establecimiento de medidas legales para garantizar que los datos personales sean tratados de manera confidencial y segura, evitando su uso indebido o su divulgación no autorizada. Al brindar a las personas el control sobre su información personal, esta legislación establece requisitos sólidos para obtener el consentimiento informado antes de recopilar, utilizar o compartir datos personales, lo que les otorga a los individuos la capacidad de decidir cómo y cuándo se utilizan sus datos.

7 Recomendaciones que considerar en un SGSI acorde a las normativas ecuatoriana y uruguaya

Con la introducción de la Ley Orgánica de Protección de Datos (LOPDP), las organizaciones están obligadas a desarrollar el concepto de protección de datos y tomar medidas para proteger los datos personales.

Las empresas deben cumplir con los requisitos operativos y de seguridad de la información interna. Combinar la protección de datos y la seguridad de la información suena complicado, pero también ofrece una serie de beneficios para las empresas.

Actualmente, uno de los problemas que enfrentan las empresas es la organización de la seguridad de la información y más aun hablando del aumento de delitos informáticos graves; a pesar de ello, la norma internacional ISO 27001 brinda buenas prácticas para implementar un Sistema de Gestión de la Información que puede minimizar los riesgos relacionados con los activos de información; es decir, prevenir y eliminar oportunamente estos riesgos y vulnerabilidades.

La implementación de un Sistema de Gestión de Seguridad de la Información traerá importantes beneficios a una empresa u organización, entre ellos: Mayor confianza de la entidad en la sociedad en general, mayor transparencia y seguridad en el tratamiento de la información. Es más fácil celebrar contratos comerciales con mayores garantías, roles y responsabilidades ya que estos son definidos de forma clara.

La gestión eficaz de la información no es una tarea fácil. Sin embargo, es de suma importancia contar con un sistema que asegure la integridad, confidencialidad y disponibilidad de los activos de información y, al mismo tiempo, reduzca los riesgos de seguridad de la información.

Toda organización que desee implantar un SGSI debe ser proactiva y comprometida con el establecimiento de medidas de seguridad para el tratamiento de la información, velando por su integridad y cumpliendo continuamente con la legislación aplicable en materia de protección de datos personales de las personas.

La LOPDP evita el uso masivo de datos personales, especialmente los clasificados como confidenciales, estrictamente confidenciales o privados, y tiene por objeto asegurar y salvaguardar el tratamiento de los datos de las personas y sus derechos fundamentales; en especial el derecho a la honra y a la intimidad.

La ley también establece que existan dos responsables: uno encargado del tratamiento y otro de seguridad de los datos personales; es decir, dentro de una estructura de seguridad de la información existen ambos roles o puestos, los cuales también están claramente delimitados en sus responsabilidades.

El conocimiento o implantación de un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 asegura a las empresas el cumplimiento de lo dispuesto en la LOPDP por dos motivos básicos:

Se debe registrar un inventario de los activos de información de la organización e indicar el debido tratamiento que incluya herramientas que permitan garantizar su acceso, de acuerdo con su clasificación y criticidad.

Se deben establecer procesos, manuales y procedimientos para certificar el cumplimiento de todas las leyes aplicables.

Responsabilidad de la alta dirección. Para que el proyecto produzca los resultados esperados, es fundamental el apoyo, soporte, patrocinio y participación de la alta

dirección. Sin un respaldo formal, es complicado desarrollar y demostrar cumplimiento en una implementación de SGSI.

Cada organización es un mundo separado. Ya sea que pertenezcan a una misma línea de negocio o al mismo grupo empresarial, cada entidad tiene su propio entorno de control y riesgos de seguridad de la información. Se debe prestar atención a la comprensión de los requisitos de seguridad y gestión de riesgos de la institución.

Determinación correcta del alcance. Es primordial determinar un alcance realizable del sistema de gestión. Los esfuerzos para implementar un sistema de gestión difieren de aquellos que involucran todos los procesos de la organización a diferencia que incluya solo dos o tres procesos relevantes. Asimismo, es mejor comenzar con unos pocos procesos y ampliar gradualmente el alcance del SGSI en el transcurso que la seguridad de la información se vuelve más madura.

El Sistema de Gestión de Seguridad de la Información es de la empresa. Ocasionalmente, las compañías que convienen servicios de consultoría para ayudar a definir e implementar un sistema de gestión cometen el gran error de asignar todas las tareas a los consultores sin participar activamente en el desarrollo del proyecto.

Análisis de brechas (GAP). Este es un estudio introductorio que permite averiguar cómo se está desempeñando la organización en términos de seguridad de la información en relación con las mejores prácticas. Para ello se utilizan los criterios establecidos en las normas o estándares. El análisis identifica la diferencia entre el desempeño real y el deseado.

Definir el nivel de entendimiento que la organización o empresa posee en protección de datos y si se han abordado acciones al respecto. Para explicar dicho nivel de conocimiento en esta fase inicial se utiliza un documento denominado “lista de verificación en materia de protección de datos”

Con dicha lista se pretende conocer:

- Si existe una cultura de seguridad de la información.
- Las diferentes áreas/empleados que tienen acceso a los datos personales.
- Fin del tratamiento.
- Tecnologías utilizadas en el tratamiento de los datos personales.
- Sistema de tratamiento (papel, digital o mixto).
- Categoría de datos personales tratados.
- Medidas organizativas y técnicas de seguridad utilizadas.
- Procedimientos para restaurar y respaldar la información.

Este documento, por lo tanto, permite un acercamiento en materia de protección de datos y, a su vez, sirve como una orientación para el encargado de protección de datos o persona responsable al momento de desarrollar un programa especial de cumplimiento.

Definir el mecanismo de acceso a la información a través de autorización y control. Para identificar equipos o usuarios que se conectan a una red, servicio, sistema o aplicación, se debe implementar una política de autenticación.

Prevenir la divulgación no autorizada de información. Los acuerdos o contratos de no divulgación o confidencialidad deben firmarse y revisarse periódicamente. Estos acuerdos deben plasmar las necesidades de seguridad de la información de la organización e incluir algunos de los siguientes puntos:

- Definición de la información a proteger.
- Propietarios de la información.
- Acciones por ejecutar en caso de incumplimiento del acuerdo.
- Uso autorizado de la información confidencial.
- Condiciones para devolución o destrucción de la información una vez concluya el acuerdo.

Evitar la degradación del sistema. Al realizar un mantenimiento, revise la información confidencial del equipo y determine si el mantenimiento se debe realizar por personal interno o requiere de personal externo.

Realizar mantenimiento a los permisos de acceso a los datos y servicios autorizados. Se deben usar registros de ingresos y registros de monitoreo para permitir la auditoría de actividades de seguridad relevantes.

Desarrollar un plan de respuesta en caso de una filtración de datos. Establecer un protocolo para saber a quién se debe notificar un ataque de información. Este plan debe ser muy flexible para ayudar a mitigar las amenazas en constante evolución.

Encriptar la información. Esto será muy importante en el caso de una filtración de datos, ya que los datos robados estarán cifrados y no tendrán ningún sentido. Debe enfatizarse que la fuga de datos no solo puede derivar en la pérdida de confianza del cliente, sino también a la responsabilidad por los daños causados por los propietarios de los datos.

Diseñar y elaborar la Política de Protección de Datos. Es un documento que le permite a una organización y su órgano de gobierno establecer las bases del SGSI, definiendo sus características, alcance y objetivos. Además, es un documento que demuestra la participación de la entidad en la implementación del sistema de gestión, incluidas las medidas de control interno que permitirán identificar, prever y minimizar los riesgos que pueden ocurrir debido al incumplimiento. Los puntos esenciales que se incluyen en este documento son:

- Propósito de la Política de Protección de Datos, el propósito más fundamental de una política de protección de datos es asegurar que la organización cumpla con las leyes y regulaciones aplicables.
- Alcance de aplicación.
- Principios que rigen el tratamiento de los datos personales como: Garantizar el respeto y la privacidad de la información personal, consentimiento, finalidad, limitación de la recopilación, calidad de los datos, transparencia, transferencias internacionales, seguridad, acceso y rectificación.
- Recursos protegidos (definición, categoría de datos personales y de tratamiento).

- Registro de actividades de tratamiento, por ejemplo: activar la auditoría de trazabilidad.
- Identificación de la base legal para el tratamiento de los datos, por ejemplo: Ley Orgánica de Protección de Datos Personales, Código Orgánico Integral Penal.
- Acreditación del consentimiento. El titular acepta la política de tratamiento de sus datos personales.
- Medidas de seguridad.
- Encargados del tratamiento, como: Oficial, encargado o responsable de datos personales.
- Brechas de seguridad, como fallas en las medidas de seguridad, errores humanos, ataques cibernéticos o robo físico de dispositivos que contienen información sensible.

Especificar cualquier tratamiento de datos personales que se haya realizado. Después de definir un tratamiento, se debe describir el tratamiento en cuestión: definir los roles (encargado, responsable, destinatario, etcétera) del tratamiento, unidad del negocio que lo efectúa, propósito, base legal, sistema de tratamiento, tecnología usada, duración, normas de aplicación, medidas técnicas y organizativas establecidas.

Concientizar al personal sobre los riesgos de seguridad. Las empresas deben trabajar para crear conciencia sobre los ataques en toda la organización. Identificar amenazas de seguridad y los métodos de prevención. Es extremadamente importante que los empleados, socios, proveedores y todos los demás en la cadena de procesamiento de datos sean conscientes de los tipos de riesgos que pueden enfrentar y cómo prevenirlos.

8 Conclusiones

El presente trabajo de investigación tuvo como objetivo realizar un análisis comparativo entre la Ley Orgánica de Protección de Datos Personales de Ecuador con su ley equivalente vigente de Uruguay, enfatizando en los puntos de ciberseguridad y los delitos informáticos.

Para ello, al inicio de nuestro trabajo fue necesario tomar prestados una serie de definiciones que nos permitieron dar un contexto apropiado a la temática central de la investigación: los datos personales.

A raíz de lo mencionado, se logró identificar que la ley ecuatoriana y uruguaya tienen varias similitudes y coincidencias entre ambas. Cabe destacar, que el Reglamento Europeo también sirvió de guía y ruta al momento de bosquejar los proyectos de ley de cada país al ser el continente pionero en la identificación y hacer visible el derecho a la privacidad. Si bien este estudio se enfocó exclusivamente en dos naciones sudamericanas, fue prudente extender esta investigación hacia otras regiones.

El proyecto de Ley Orgánica de Protección de Datos Personales se convirtió en Ley Orgánica de obligatorio cumplimiento para las empresas ecuatorianas tanto del sector público como del privado con su publicación el 26 de mayo de 2021 en el Registro Oficial N. 459. La Ley viabiliza de manera práctica la protección de los datos personales como el derecho fundamental consagrado en la Constitución de la República del Ecuador.

La Ley Orgánica de Protección de Datos Personales ecuatoriana, plantea grandes retos que deben satisfacer las empresas del sector público y privado, para lo cual debían en un plazo de dos años implementar medidas jurídicas, técnicas y organizacionales encaminadas a salvaguardar los datos entregados por las personas.

La LOPDP concede a los titulares de los datos, el derecho a exigir límites en el uso de su información; es decir, le asigna el control y disposición de sus datos personales y su uso por parte de terceros.

Los altos funcionarios de las organizaciones cada vez están más involucrados, conscientes de la información y los datos de su organización y de las consecuencias penales que puede traer el incumplimiento.

Lo que está pasando hoy con nuestra información personal, privada e íntima es una realidad, sobre todo si no conocemos que nuestros datos están en todas partes, por lo que un marco de ley para proteger los datos personales es el primer paso.

Pueden aplicarse tratamientos a los datos personales; sin embargo, no se garantiza la protección de datos. Por tal motivo el ordenamiento jurídico debe asegurar la protección al momento de la recolección, si solicitan información, el solicitante es el único responsable y bajo las mismas circunstancias debe ser consciente de su almacenamiento, uso y posible transmisión.

Las recomendaciones expuestas consideramos que son un bosquejo de lo que toda organización y alta dirección deberían analizar y profundizar al momento que se plantean la implementación de un SGSI. Estas conllevarán a tener un punto de partida hasta encontrar el conjunto de recomendaciones y procedimientos que más se apeguen a las necesidades y naturaleza de cada organización.

Este trabajo puede ser de gran utilidad, aporte y ayuda para tomar medidas y recomendaciones necesarias al momento de implementar un Sistema de Gestión de Seguridad de la Información idóneo y óptimo que se apegue a la novísima Ley Orgánica de Protección de Datos Personales de Ecuador y velen por el derecho que esta ley enmarca.

Referencias

[1] T. C. Mayorga Jacome, M. Garcia Jimenez, J. F. Duret Gutierrez, J. L. Carrion Jumbo y P. V. Yarad Jeada, «Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos,» *Dominio de las Ciencias,* vol. 5, nº 1, 2019.

[2] S. A. Zamora Alvarez, «Nueva Visión del Derecho de Protección de Datos Personales en Ecuador,» enero 2022. [En línea]. Available: http://repositorio.uees.edu.ec/handle/123456789/3404. [Último acceso: septiembre 2022].

[3] Asamblea Constituyente de Ecuador, Constitución de la República del Ecuador, Registro Oficial No. 449, 2008.

[4] J. Guerron Eras, «Ecuador y su primera Ley Orgánica de Protección de Datos Personales,» GOVERTIS, 16 junio 2021. [En línea]. Available: https://dpd.aec.es/ecuador-y-su-primera-ley-organica-de-proteccion-de-datos-personales/. [Último acceso: septiembre 2022].

[5] C. Cimpanu, «Database leaks data on most of Ecuador's citizens, including 6.7 million children,» septiembre 2019. [En línea]. Available: https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/. [Último acceso: septiembre 2022].

[6] «DelitosInformáticos,» [En línea]. Available: DelitosInformáticos(**)(***)(****) - Revista - PUCP.

[7] S. Acurio del Pino, «Delitos informáticos: generalidades,» [En línea]. Available: http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599.

[8] PROTECCION DE DATOS Y DELITOS INFORMATICOS, [En línea]. Available: https://docplayer.es/43967016-Proteccion-de-datos-y-delitos-informaticos.html.

[9] Revista Seguridad 360, «Los delitos cibernéticos ejemplos reales,» [En línea]. Available: https://revistaseguridad360.com/destacados/delitos-ciberneticos-ejemplos/. [Último acceso: septiembre 2022].

[10] H. C. Gutierrez Amaya, «Top 10 de condenados por delitos informáticos: ¿quiénes fueron los primeros de la historia?,» ESET, 12 noviembre 2013. [En línea]. Available: https://www.welivesecurity.com/la-es/2013/11/12/top-10-condenados-por-delitos-informaticos-quienes-fueron-primeros-historia/. [Último acceso: septiembre 2022].

[11] I. P. Leon Galvez, B. B. Gonzalez Cueva y J. P. Montaño Guaman, «Delitos en Ecuador,» 2021. [En línea]. Available: https://www.studocu.com/ec/document/universidad-nacional-de-loja/derecho-informatico/delitos-en-ecuador-grade-22/12264134. [Último acceso: septiembre 2022].

[12] Fiscalía General del Estado, «Los delitos informáticos van desde el fraude hasta el espionaje,» junio 2015. [En línea]. Available: https://www.fiscalia.gob.ec/los-

delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/. [Último acceso: septiembre 2022].

[13] «Protección de datos,» [En línea]. Available: https://teuno.com/blogs/ley-organica-de-proteccion-de-datos.

[14] «GlobalSuite,» [En línea]. Available: https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/.

[15] F. N. Roldan Carrillo, «Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador,» *USFQ Law Review,* vol. 8, nº 1, pp. 175-202, mayo 2021.

[16] «Direccion Nacional de Registros Publicos,» [En línea]. Available: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/.

[17] «Deloitte,» [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/legal/FL%20VF.pdf.

[18] M. Cornejo Velazquez, M. Garcia Munguia, I. M. Gonzalez Ceron y M. N. Guerrero Rubio, «Principios de Seguridad Informática en Sistemas de Información,» *xikua,* vol. 3, nº 6, 5 julio 2015.

[19] Equipo editorial Etecé, «Concepto,» 5 agosto 2021. [En línea]. Available: https://concepto.de/ley-organica/. [Último acceso: 5 septiembre 2022].

[20] Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, Quito, Pichincha, 2021.

[21] Asamblea General de Uruguay, Ley 18331 Protección de Datos Personales y acción de "Habeas Data", 2008.

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

[23] J. Erickson, Hacking: the art of exploitation, Segunda ed., San Francisco, California: No Starch Press, 2008.

[24] C. C. Palmer, «Ethical hacking,» *IBM Systems Journal,* vol. 40, pp. 769-780, 2001.

[25] A. Guevara Soriano, «Hacking ético: mitos y realidades,» *Revista .Seguridad,* nº 12, 16 enero 2012.

[26] X. Jubeto Lopez, «Diseño e implementación de una plataforma Cyber Range CTF (Capture The Flag) contra objetivo ETSI OSM,» 23 noviembre 2021. [En línea]. Available: http://hdl.handle.net/10810/54017. [Último acceso: 6 septiembre 2022].

[27] P. D. D. D. P. D. P. Y. P. D. D. P. E. L. AMÉRICAS, «Comité Jurídico Interamericano (CJI),» marzo 2012. [En línea]. Available: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf. [Último acceso: 6 diciembre 2022].

[28] Universidad Andina Simón Bolívar - Observatorio de Ciberderechos y Tecnosociedad, «Protección de datos,» [En línea]. Available: https://www.uasb.edu.ec/ciberderechos/proteccion-de-

datos/#:~:text=La%20protección%20de%20datos%20personales,directiva%2095%2F46%2FCE. [Último acceso: 6 diciembre 2022].

[29] M. P. Canales y M. Bordachar, «Protección de datos personales en Ecuador: El momento es ahora,» 22 enero 2021. [En línea]. Available: https://www.derechosdigitales.org/15138/proteccion-de-datos-personales-en-ecuador-el-momento-es-ahora/. [Último acceso: 6 diciembre 2022].

[30] PROTECCIÓN DE DATOS Y PREVENCIÓN DE DELITOS, «Agencia Española de Protección de Datos,» [En línea]. Available: https://www.aepd.es/es. [Último acceso: 6 diciembre 2022].

[31] J. V. Enriquez Herrera y Y. C. Alvarado Salinas, «LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO,» *SATHIRI: Sembrador,* nº 8, pp. 171-194, 1 junio 2015.

[32] M. Pecoy Taque, «EL PROYECTO DE LEY URUGUAYO DEL AÑO 2021 QUE PRETENDE LA TIPIFICACIÓN DE LOS CIBERDELITOS EN URUGUAY,» 16 agosto 2021. [En línea]. Available: https://laleyuruguay.com/blogs/novedades/el-proyecto-de-ley-uruguayo-del-ano-2021-que-pretende-la-tipificacion-de-los-ciberdelitos-en-uruguay. [Último acceso: diciembre 2022].

[33] Diario Correo de Punta del Este, «Diputado Cal continúa trabajando en proyecto de ley sobre ciberdelitos y prepara otro sobre protección de datos,» 4 septiembre 2022. [En línea]. Available: https://correopuntadeleste.com/diputado-cal-continua-trabajando-en-proyecto-de-ley-sobre-ciberdelitos-y-prepara-otro-sobre-proteccion-de-datos/. [Último acceso: diciembre 2022].

[34] Dirección de Comunicación Social, «Ley de Protección de Datos Personales,» [En línea]. Available: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/. [Último acceso: septiembre 2022].

[35] P. d. L. e. m. d. p. d. d. personales, «Deoitte Legal,» julio 2021. [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/legal/Proyecto%20de%20Ley%20Cuidados%20Legal.pdf.