FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE LOS ASPECTOS TÉCNICOS DEL MARCO REGULATORIO PARA LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR.

Autor

Jaily Stefan Remache Arias

Año
2019

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE LOS ASPECTOS TÉCNICOS DEL MARCO REGULATORIO PARA LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR.

"Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones"

Profesor guía
Mg. Edwin Guillermo Quel Hermosa

Autor
Jaily Stefan Remache Arias

Año
2019

DECLARACION PROFESOR GUÍA

"Declaro haber dirigido el trabajo, de los aspectos técnicos del marco regulatorio para la protección de datos personales en Ecuador, a través de reuniones periódicas con el estudiante Jaily Stefan Remache Arias, en el semestre 201920, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Edwin Guillermo Quel Hermosa

Magister en Gerencia de Redes y Telecomunicaciones

CI. 171872689-4

DECLARACIÓN PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, de los aspectos técnicos del marco regulatorio para la protección de datos personales en Ecuador, de Jaily Stefan Remache Arias, en el semestre 201920, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Nathaly Verónica Orozco Garzón
Doctora en Ingeniería Eléctrica en el Área de
Telecomunicaciones y Telemática
CI. 172093858-6

DECLARACION DE AUTORIA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Jaily Stefan Remache Arias

CI: 1003288139

AGRADECIMIENTOS

Gracias en especial a mis abuelos José y Zoila; siempre estarán en mi corazón, nunca olvidaré todo su cariño y amor hacia mí.

A mi padre, un gracias enorme por haber compartido y apoyado en mis triunfos y tropiezos en esta etapa.

A mi abuela Ana, gracias por ser otro de los pilares importantes en mi vida, su esfuerzo en la vida es un ejemplo para mí.

DEDICATORIA

Querida mamá, cada una de estas páginas es dedicado a todo tu sacrificio y lucha por enseñarme a ser mejor cada día; mi completa admiración a una mujer como tú.

Gracias por todo lo que has hecho y haces por mí. Me has hecho reír, me has secado las lágrimas. Me has visto triunfar, me has visto caer. Tu corazón sabe comprender cuando necesito una amiga.

Tu esfuerzo y tu amor me han dirigido por la vida, y me han dado las alas que necesitaba para volar; y es solo el comienzo…

Mi amor por ti será eterno. Te quiero.

RESUMEN

Se define como datos personales, la información de carácter personal que debe ser protegida para evitar su divulgación o manipulación sin la autorización del usuario; en Ecuador se ha desarrollado una propuesta para la Protección de Datos Personales la cual en la actualidad se encuentra en revisión para su aprobación, por lo que el presente documento tiene como finalidad emitir recomendaciones en relación a los aspecto técnicos que debe incluir dicha propuesta, para lo cual en primera instancia se realizó una revisión de la normativa mundial en torno al tema de protección de datos y en especial de las normativas en Ecuador y América latina, de igual forma se analizó la propuesta de la *Ley Orgánica de la Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales,* presentada por la Asamblea Nacional de Ecuador en el año 2016, en la cual se detectó una serie de vacíos regulatorios, por lo cual se recomendó incluir varios artículos que regulen lo referente a las responsabilidades de los diversos entes involucrados en el tratamiento de los datos y la aplicación de mecanismos técnicos para asegurar la anonimación de datos en los sistemas de telecomunicaciones, los resultados obtenidos servirán de base y sustento técnico para los entes reguladores.

Palabras clave: Datos personales, Privacidad por Diseño (PbD), Tecnologías para mejorar la privacidad (PET), anonimización, sistemas de información.

ABSTRACT

Personal data is defined as personal information that must be protected to prevent its disclosure or manipulation without the authorization of the user; In Ecuador, a proposal has been developed for the Protection of Personal Data, which is currently under review for approval, so the purpose of this document is to issue recommendations in relation to the technical aspects that such proposal must include. which in the first instance was a revision of the global norm around the topic of data protection and especially of the regulations in Ecuador and Latin America, likewise the proposal of the Organic Law of the Protection of Rights was analyzed to the Privacy and Privacy of Personal Data, presented by the National Assembly of Ecuador in 2016, in which a series of regulatory gaps were detected, for which it was recommended to include several articles that regulate the responsibilities of the various entities involved in the processing of data and the application of technical mechanisms to ensure the anonymity of data in telecommunication systems, the results obtained will serve as the basis and technical support for the regulatory entities.

Keywords: Personal data, Privacy Enhancing Technologies (PET), Privacy by Design (PbD), anonymization, information systems

ÍNDICE

1. CAPITULO I. INTRODUCCIÓN

1.1 Antecedentes

El vertiginoso progreso de las tecnologías aporta grandes beneficios a las sociedades, y a su vez representa desafíos propios de la evolución de los sistemas de comunicación e información; entre ellos nuevas formas de transgresión de derechos fundamentales de los ciudadanos.

En la actualidad como resultado de los avances tecnológicos y los mecanismos de comunicación, los datos asociados a nuestra vida privada se encuentran disponibles en las redes de comunicación; las personas en general aportan información personal al usar las herramientas disponibles en Internet, como redes sociales, comercio electrónico, comunicación electrónica, entre otros.

La disponibilidad de datos personales en la redes ha conquistado gran relevancia, dado que dicha información adquiere un poder especial ante las instituciones públicas y privadas; esto ha generado que este tema se convierta en un área de preocupación para las autoridades nacionales e internacionales, las cuáles se han dado a la tarea de adecuar las disposiciones legales que actualmente existen para la Protección de Datos Personales, dado que el manejo indebido de la información da origen a la violación de los derechos fundamentales, entre los que se mencionan el derecho a la privacidad, intimidad y dignidad humana.

Esto ha originado la necesidad de crear y configurar reglamentos o normas con rapidez y de forma continua, a fin de mantener las garantías constitucionales y legales mediante un sistema de amparo y protección a aquellas personas o entes que se puedan ver afectados por las innovaciones tecnológicas y el uso de datos personales.

La Unión Europea en el convenio 108 de 1981 del Consejo de Europa y la Directiva Europea 95/46 1995 estableció, que los principios mínimos en Protección de Datos que deben tener los países para ser considerados como garantes de la transferencia internacional de datos son: limitación de la finalidad, calidad de datos y proporcionalidad, transferencia, seguridad, acceso, restricción y oposición (Consejo de Europa, 1981).

En la actualidad los países del mundo tienen un profundo interés en regular la protección de datos personales con el fin de proteger los derechos de sus ciudadanos, y fomentar el desarrollo de empresas que administren información por medios tecnológicos. La protección de datos personales es fundamental para desarrollar gobiernos electrónicos con políticas coherentes, en los cuales el lenguaje jurídico debe estar a la par del desarrollo tecnológico.

La Constitución de la República del Ecuador, garantiza el acceso de los datos personales (Habeas Data), haciendo énfasis en el manejo automatizado de la información. La Constitución en su art. 66, núm.19 instituye la protección de datos personales:

> "El derecho a la protección de datos de 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 o información requerirán la autorización del titular o el mandato de la ley". (Gobierno de Ecuador, 2008, pág. 49)

La directora nacional de Registro de Datos Públicos (DINARDAP), Mgs. Lorena Naranjo Godoy (2017), explicó el rol que tiene el "Estado como responsable de los datos personales", indico que todo este potencial (datos personales), que mueve las economías y que permite tomar mejores decisiones, no ha podido ser regulada en Ecuador. "Nuestro país es el claro ejemplo de normativa con enfoque sectorial, es decir, existen varias normas dispersas que aparecen en

leyes específicas", a su criterio, los principales retos que "tenemos como Estado es no desactualizarnos más aún de lo que estamos para no aislarnos a escala internacional, y generar la Ley de Protección de Datos" concluyo estableciendo que: Ecuador necesita una Ley de Protección de Datos Personales con visión técnica. (Información tomada de la página web DINARDAP, (2017).

Para la correcta protección de los datos personales de los usuarios, es imprescindible que estos valoren el tipo de datos que publican en su perfil. Además, se considera crucial, que las organizaciones públicas y privadas realicen, desde el momento en que se produce el registro y se crea el perfil de usuario, labores de información, formación y concienciación sobre los peligros de la publicación excesiva de contenidos (Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2009).

En base a lo anteriormente expuesto, se propone realizar el presente trabajo a fin de determinar si existen vacíos regulatorios en Ecuador o que aspectos de la regulación actual son necesarios modificar para ajustarlos, con la finalidad de realizar un marco de recomendaciones que podrán ser aplicables a la normatividad vigente. Además, los resultados obtenidos podrán servir como fuente de consulta para profesionales y estudiantes de derecho, ya que aportará una visión técnica a la normativa.

1.2 Alcance

Este proyecto inicia con la revisión sobre las tecnologías de telecomunicaciones para la transmisión de información disponibles en la actualidad y los aspectos técnicos que influyen en la filtración de datos personales de usuarios hacia la red de Internet sin la respectiva aprobación.

La normativa de protección de datos que presenta el estado ecuatoriano tendrá que ser revisada estudiando su bibliografía completa y realizando la comparación con los países del mundo líderes en este tema.

Del mismo modo, los riesgos sobre los datos personales a los que se enfrentan en la actualidad las personas que utilizan las tecnologías de telecomunicaciones deben ser identificados y analizados para poder canalizar los mecanismos necesarios para controlarlos y regularlos con el fin de ofrecer protección al usuario final en los que respecta a privacidad de sus datos. Además, se determinará las responsabilidades de los entes involucrados en los tratamientos de datos dentro de estas tecnologías.

Finalmente, en base a las variables previamente analizadas se propondrán recomendaciones para el control y regulación de datos personales en el Ecuador. El presente trabajo servirá de aporte para los entes regulatorios en Ecuador incorporando una visión técnica al sistema normativo por desarrollar.

1.3 Justificación

Este proyecto tiene la finalidad de presentar los primeros pasos requeridos para la formulación de una normativa que regule los aspectos técnicos en los sistemas relacionados a la protección de datos de los ciudadanos ecuatorianos.

En la actualidad, las tecnologías para la transmisión de información permiten a las empresas obtener grandes volúmenes de información de Internet y otras fuentes, utilizando estos datos para su beneficio creando entre otras opciones, perfiles comerciales. Esta manipulación de datos puede ser perjudicial para los ciudadanos que desconocen el uso que se le da a su información personal, violando su derecho a la privacidad y seguridad.

El uso de nuestros datos personales sin nuestro consentimiento es considerado un delito. Es responsabilidad del estado promover normas o leyes que protejan

a sus ciudadanos, por lo que en la actualidad los gobiernos del mundo se encuentran en constante evaluación y emisión de normativas a fin de regular lo relacionado con las Tecnologías de Telecomunicaciones.

En el desarrollo del presente trabajo se identificarán los cuatro conceptos clave de seguridad de la información: confidencialidad, autenticación, integridad y no repudio. La confidencialidad es la propiedad que asegura que sólo aquellos que están autorizados tendrán acceso a la información. A menudo esta propiedad se conoce también con el nombre de privacidad. La integridad es la propiedad que asegura la no alteración de la información. Esta alteración puede ser, por ejemplo, insertar, borrar o sustituir información, la autenticación es la propiedad que hace referencia a la identificación. Se trata del punto de unión entre la información y el emisor de esta información. El no repudio es la propiedad que impide que alguna de las partes niegue algún compromiso o acción adoptados con anterioridad (Poch, 2004).

Con el desarrollo del presente proyecto, se busca avanzar en la regulación para la protección de los datos que son administrados por las Tecnologías de Comunicación, los resultados obtenidos podrán servir de base para que los entes reguladores desarrollen y propongan leyes en torno a este problema universal, y finalmente colocar a Ecuador a la cabeza de los avances regulatorios en materia tecnológica, además representará un aporte para la Universidad como instrumento de consulta en lo relacionado a la protección de datos personales.

1.4 Objetivos

1.4.1 Objetivo general

“Análisis de los aspectos técnicos del Marco Regulatorio para la Protección de Datos Personales En Ecuador”

1.4.2 Objetivos específicos

- Analizar los aspectos técnicos en los sistemas de comunicación relacionado con la protección de datos personales.
- Estudiar el marco regulatorio que existe a nivel nacional e internacional para la protección de datos personales.
- Identificar los riesgos para la protección de datos personales que representa los avances tecnológicos en los sistemas de comunicación.
- Desarrollar una recomendación sobre los aspectos técnicos para la protección de datos personales en el Ecuador.

2. CAPÍTULO II. ANÁLISIS DE LOS ASPECTOS TÉCNICOS EN LOS SISTEMAS INFORMÁTICOS RELACIONADO CON LA PROTECCIÓN DE DATOS

El presente capítulo describe los aspectos más importantes relacionados a las tecnologías de los sistemas de información que están involucrados en la protección de datos personales.

2.1 Definición de dato

El concepto de “Dato” proveniente del latín “datum” que significa “lo que se da”, es decir, un dato es la información que se aporta de forma numérica o alfabética. Los datos refieren contextos que por sí solos no reportan información relevante; acompañando de alguna experiencia es cuando aporta algún valor como por ejemplo el número de cedula, una cuenta de correo electrónico, el número de cuenta bancaria, etc (Aristizábal & Arias, 2011).

2.2 Dato personal

El dato personal es información contenida en la ficha o cédula de identidad de una persona, como el nombre, número de identificación, fecha de nacimiento, etc., se considera también toda información que permite individualizar e identificar a una persona (Chen, 2010).

2.2.1 Tipo de datos personales

Existen algunas clasificaciones de los datos según los autores. La principal clasificación está determinada de la siguiente manera:

a) Dato anónimo: Se llama así al dato estadístico o general que no personaliza ni permite la personalización.
b) Dato nominativo: Es aquel que está referido a una persona determinada. Lo dividimos de acuerdo a como sea la forma de acceso a la identificación de la persona. Pueden ser de dos tipos:

    - Directos: cuando lo identifica sin necesidad de proceso alguno.
    - Indirectos: cuando permite la identificación, pero no lo identifica en forma directa, sino agrupando datos. Reinoso (2014)

A su vez el dato nominativo se puede clasificar en:

- Dato nominativo sensible: es aquel que afecta o puede afectar la intimidad como por ejemplo una información de diagnóstico médico.
- Dato nominativo no sensible: es aquel que si bien es personal, es destinado a ser público, por ejemplo número de documento de identidad. Reinoso (2014)

El dato nominativo sensible, es el protagonista de esta investigación, ya que son los datos personales que son propios de la intimidad de la persona y se entiende que por su naturaleza deben ser reservados y por esto para su recolección y manejo se necesita una regulación proteccionista.

2.3 Datos personales sensibles

Se considera datos de naturaleza sensible a aquella información de carácter personal:

a) Que pueda generar alguna afectación a las personas en el círculo íntimo del interesado;
b) el uso inapropiado de la misma pueda generar:
    - Discriminación de alguna naturaleza
    - Generar algún tipo de peligro para el interesado. Santos (2005)

Los datos personales sensibles son aquellos relacionados a la ideología, religión, creencias, origen racial, vida e inclinación sexual, estado de salud; y se refiere a ellos de la siguiente manera:

2.3.1 Ideología

Dicha información se refiere a un conjunto de ideas que tiene el individuo respecto a la realidad o al sistema, y tiene que ver por ejemplo con la inclinación política o filiaciones sindicales.

2.3.2 Creencia

Tiene relación con las convicciones del individuo que pueden variar con respecto a los demás. Éstas no dejan de ser información personal y por tanto no se puede divulgar sin consentimiento del afectado.

2.3.3 Religión

La convicción religiosa, viene dada por la libertad de culto y claramente nadie debe ser privado de sus prácticas religiosas y tampoco divulgar sus creencias y cultos si no lo cree necesario.

2.3.4 Origen racial

Son relativos a la pertenencia de una persona a un pueblo o nación, es decir, son los datos culturales, sociales y físicos que definen a un grupo social con relación a la persona. Este tipo de datos son delicados por el tema de posible discriminación o segregación racial que se ha vivido en muchas sociedades a lo largo de la historia, por ello la protección a esta información.

2.3.5 Vida o inclinación sexual

Los datos acerca de la vida sexual son bastante variados, pero entendemos que la sexualidad es el ámbito más profundo de la intimidad por lo que incluye datos acerca de la actividad sexual, la ausencia de dicha actividad, preferencias sexuales y toda la información acerca de este tema.

2.3.6 Salud

Estos datos hacen referencia no solo a las enfermedades que padezca el individuo sino también a diagnósticos y tratamientos, el autor nos aclara que incluso un informe médico psicotécnico que contenga la categoría “apto” o “no apto” se considera un dato de salud. Son los datos que se refieran al estado de salud pasada, presente o futura, y de la salud física o mental, y deben extenderse a adicciones como la drogadicción o alcoholismo. Santos (2005)

2.4 Tecnologías de información

La tecnología de la información se refiere a los sistemas automatizados para almacenar, procesar y distribuir información. Típicamente, esto implica el uso de computadoras y redes de comunicación. La cantidad de información que se puede almacenar o procesar en un sistema de información depende de la tecnología utilizada. La capacidad de la tecnología ha aumentado rápidamente en las últimas décadas, de acuerdo con la Ley de Moore. Esto es válido para la capacidad de almacenamiento, la capacidad de procesamiento y el ancho de banda de la comunicación. Ahora somos capaces de almacenar y procesar datos en el nivel de exabyte (Barinas, 2013). A su vez, la tecnología de la información consiste en un complejo sistema de prácticas sociotécnicas, y su contexto de uso constituye la base para analizar su impacto en la privacidad. Entre los principales desarrollos en las tecnologías de información se encuentran:

2.4.1 Internet

Un tema importante en la discusión sobre la privacidad en Internet gira en torno al uso de *cookies*. Las *cookies* son pequeños fragmentos de datos que los sitios web almacenan en la computadora del usuario para permitir la personalización del sitio. Sin embargo, algunas *cookies* se pueden usar para rastrear al usuario en múltiples sitios web (*cookies* de rastreo) (Domingo, 2014).

De la misma forma, el reciente desarrollo de la computación en la nube aumenta las muchas preocupaciones de privacidad. Anteriormente, la información acerca de datos y programas de los usuarios se almacenaba de forma local, evitando así de cierto modo que los proveedores o desarrolladores de programas tuvieran acceso a los datos y las estadísticas de uso (Barriuso, 2009).

En la computación en la nube, tanto los datos como los programas están en línea (en la nube), y no siempre está claro para qué se utilizan los datos generados por el usuario y los generados por el sistema (Barinas, 2013). En general, los servicios de Tecnologías de la Información (TI) tienen más y diferentes problemas de privacidad que los productos de TI, esto debido a los controles y tecnologías de protección de datos que se aplican a los productos, los cuales no pueden ser replicados para los servicios, además de considerar el volumen el cual en el caso de los servicios es supremamente mayor que para los productos y la ubicación de los datos que manejan cada uno.

2.4.2 Medios sociales

La web interactiva, conocida como Web 2.0, donde los usuarios generan gran parte del contenido por sí mismos, plantea desafíos adicionales. Como ventaja fundamental es que permite a los usuarios interactuar y colaborar entre sí (Barriuso, 2009).

Las principales características de la Web 2.0 son:

- Extensión de la red; la cual se ha convertido en un punto de publicación y acceso a la información, que proviene de múltiples fuentes de información, en un régimen de descentralización. Es decir, que ya no existe de forma unilateral (generada unilateralmente por los editores de información, de acuerdo con el modelo tradicional de publicación).
- Interoperablidad entre los distintos recursos; consecuente del punto anterior, y donde el usuario se convierte en partícipe en la generación de contenidos.

  En otras palabras, el usuario deja de lado su condición de usuario pasivo o unilateral en sentido estricto, y forma parte de la red en una doble vertiente: como usuario y como generador de contenido y, por tanto, de información. De hecho, estos usuarios de la Web 2.0 ya

empiezan a identificar como ‘prosumidores’, entendiendo que ya no solo ‘consumen’ contenidos, sino que además los ‘producen’.

- Pluralidad de formatos; el contenido disponible no consiste únicamente en texto, sino que permite compartir la información a través de otros muchos formatos como imagen, vídeo, música, etc.
- Herramienta de comunicación masiva e inmediata; permite la comunicación entre distintos focos de información de manera instantánea. Así, los contenidos generados pasan a estar disponibles para el resto de usuarios de forma casi inmediata. Además, la web 2.0 permite a los usuarios seleccionar qué contenido quieren ver y bloquear la información que no les interesa (Guilayn & Ruiz, 2016).

2.4.3 Web 3.0

Denominada ‘web semántica’, la ‘web geoespacial’, la ‘web 3D’ o ‘*data web’*; se basa en gran medida, en los elementos, herramientas y actitudes que mejor y mayor acogida han tenido entre los usuarios y, con ayuda de las nuevas tecnologías, los mejora y perfecciona para lograr un mejor resultado (Salazar, 2011).

La idea radica, más allá de que los usuarios proporcionen información y la sometan a sistemas etiquetados comprensibles que faciliten la búsqueda, en que el control, procesamiento de información, resolución de problemas o deducciones lógicas sean realizados por el ‘*software*’ dejando de lado al usuario como responsable de estas actividades (Berners, 2016).

La Web 3.0 facilita la accesibilidad de las personas a la información, sin depender de qué dispositivo use para el acceso a ella. Es decir, se trata de una herramienta con la que interactuar para conseguir resultados más allá del hecho de compartir información. Esta información será también compartida por cada persona de una forma inteligible y de provecho para ella y sus necesidades en cada circunstancia, y que, además, estará diseñada bajo parámetros de rendimiento eficiente, optimizando los tiempos de respuesta,

optimizando los consumos energéticos globales del sistema, optimizando las exigencias técnicas y tecnológicas, optimizando los conocimientos y capacidades que se requiera al usuario ya que es una web más intuitiva, humanizada (Salazar, 2011).

2.5 Tecnologías asociadas a la filtración de información

Los enfoques de seguridad tradicionales, como los *firewalls*, no pueden proteger los datos contra fugas. Los sistemas de prevención de pérdida de datos (del inglés, *Data Loss Prevention*, DLP) son soluciones que protegen que los datos confidenciales no lleguen a caer en manos no confiables.

La fuga de información ocurre cuando se revelan datos confidenciales a partes no autorizadas, ya sea intencionalmente o no. Los datos filtrados pueden causar graves amenazas a las personas o empresas. Las soluciones DLP ayudan a identificar, monitorear, proteger y reducir los riesgos de fuga de datos confidenciales. Las tecnologías tradicionales tienen como definición proteger los datos desde el exterior, mientras que el sistema DLP se concentra en la protección de datos desde el interior.

2.5.1 Tecnologías tradicionales

Las técnicas tradicionales utilizan el método de inspección profunda de paquetes (del inglés, *Deep Packet Inspection*, DPI); el cual examina el paquete, detecta las anomalías en el tráfico y alerta al administrador. Los siguientes pasos describen cómo funciona esta arquitectura:

a) El intérprete de lenguaje de definición de patrones usa firmas que se pueden escribir para detectar y prevenir protocolos conocidos y desconocidos. La DPI reensambla los paquetes del Protocolo de Control de Transmisión (TCP) que llegan fuera de servicio.

b) El pre-procesamiento del motor de DPI implica la normalización de la carga útil del paquete. Por ejemplo, una solicitud de Protocolo de Transferencia de Hipertexto (HTTP) puede estar codificada en un Localizador Uniforme de Recursos (URL) y, por lo tanto, la solicitud se decodifica en URL para realizar una coincidencia de patrones correcta en la carga útil.
c) Los postprocesadores del motor de inspección profunda de paquetes realizan acciones que pueden simplemente pasar el paquete sin modificaciones, o podrían dejar caer un paquete o incluso restablecer una conexión TCP.

2.5.1.1 Los Sistemas de Detección de Intrusos (IDS) y Sistemas de Prevención de Intrusos (IPS)

Los IDS son un tipo de dispositivo o aplicación de *software* que controla las redes o las actividades del sistema en busca de actividades maliciosas (Olguín, Rivera, & Pérez, 2016).

Por otro lado, los IPS monitorean las redes y las actividades del sistema en busca de actividades maliciosas, actúa intentando bloquear o detener las actividades maliciosas detectadas. Además, los sistemas IPS son una expansión de los Sistemas de Detección de Intrusos porque monitorean el tráfico de la red. También, realizan actividades para detectar situaciones maliciosas y, pueden prevenir o bloquear las intrusiones detectadas (Capo, 2015).

Los Componentes de IDS / IPS Se pueden usar para buscar ataques, rastrear los movimientos de los piratas informáticos y alertar a un administrador de los ataques en curso, y constan de más de una aplicación o dispositivo de hardware. La mayoría de IDS / IPS consta de las siguientes partes:

- Sensores de red: detectan y envían datos a los sistemas.

- Sistema de monitoreo central: procesa y analiza los datos enviados desde los sensores.
- Análisis de informes: ofrece información sobre cómo contrarrestar un evento específico (Olguín, Rivera, & Pérez, 2016).

De la misma forma, existen variantes de IDS/IPS que mejoran su funcionalidad:

- Los sistemas de detección de intrusos basados en red (del inglés, *Network Intrusion Detection System*, NIDS / NIPS) se encargan de verificar los paquetes en la red y descubrir los datos en un intento por reconocer un ataque.
- Los sistemas de detección de intrusos basados en host (del inglés, *Host-based Intrusion Detection System*, HIDS / HIPS) realizan el monitoreo del tráfico en un sistema específico; es excelente para detectar o prevenir el acceso de actividades no autorizadas, ya que se encarga de observar el estado de un sistema o componente, verificando que todo el comportamiento corresponda a lo esperado (Olguín, Rivera, & Pérez, 2016).

2.5.1.2 Anti-Malware

El software malicioso es un software diseñado para dañar las operaciones de la computadora, recoger datos confidenciales y obtener acceso no autorizado al sistema informático. El *malware* puede presentarse y atacar en forma de virus, gusanos, troyanos, software espía, puertas traseras y kit de raíz (Ramírez, García, & Bocarando, 2016).

El *malware* tiene dos categorías:

- *Malware* que modifica los recursos como memoria, código BIOS, expansiones de dispositivos, etc.

- *Malware* que modifica los recursos que son dinámicos por naturaleza, como por ejemplo secciones de datos o la modificación de algunos punteros de función en algunas estructuras de datos del Kernel, para que el código de los atacantes se ejecute en lugar del sistema o aplicación original (Latorre, 2014).

El gusano de red es un programa de autopropagación que es difundido a través de una red, generalmente Internet. A diferencia de los virus, es posible que no dependan de otros programas o acciones de la víctima (como abrir un archivo adjunto de correo electrónico infectado o hacer clic en un enlace web para un sitio web de malware) para la replicación, difusión o ejecución (Ramírez, García, & Bocarando, 2016).

Por su parte, el caballo de Troya o troyano es un programa destructivo que se hace pasar por un programa benigno, por ejemplo cuando se hace clic en los *pop-ups* (ventanas emergentes) que aparecen en los navegadores o al abrir fotos y archivos recibidos de desconocidos vía correo electrónico.

El software del caballo de Troya se instala en la computadora de un usuario cualquiera y en el momento de abrir un archivo adjunto de correo electrónico o archivo de computadora que contiene el troyano, se le redirecciona hacia un sitio web desde el cual el troyano es automáticamente descargado. (Chávez & Espinoza, 2017)

El código malicioso incorporado es un tipo de lógica maliciosa incrustada en un programa ejecutable válido por su desarrollador, integrador, distribuidor o instalador. Con mayor frecuencia una bomba lógica, bomba de tiempo o troyano. (Chávez & Espinoza, 2017)

Para evitar los problemas anteriormente desarrollados es necesario poseer un *anti-malware*. Este software brinda protección a computadoras y sistemas contra *malware*, virus, otros programas dañinos. Además, funciona en un

entorno de tiempo real de manera muy eficaz, pero solo busca amenazas externas, mediante el escaneo y la validación de la firma.

2.5.1.3 Firewalls

Los *firewalls* son dispositivos o software que permiten o niegan las transmisiones de red basadas en un conjunto de reglas (regla de acceso) y se utilizan para proteger las redes de accesos no autorizadas mientras permiten la comunicación legal, que ayuda a mantener la red segura y su objetivo principal es controlar el tráfico entrante y saliente de las redes analizando el paquete de datos y determinando si se debe permitir o no a través de él. (Chávez & Espinoza, 2017)

2.5.2 Sistema de prevención de pérdidas (DLP)

Es una solución diseñada para detectar posibles incidentes de violación de datos en forma oportuna, la tecnología DLP están diseñada para detectar y prevenir el uso no autorizado y la transmisión de datos confidenciales. Además, se puede configurar para identificar el monitor y proteger los datos en uso, los datos en movimiento y los datos en reposo (Torres, 2017).

Las soluciones DLP distinguen tres fases de datos a lo largo de su ciclo de vida: datos en reposo (DAR), datos en movimiento (DIM) y datos en uso (DIU).

a) Los datos en reposo (DAR) se definen como todos los datos en el almacenamiento de la computadora. Para evitar el acceso, el robo o la alteración de este tipo de información, se utilizan comúnmente, medidas de seguridad como el cifrado de datos y el control de acceso.
b) Un requisito previo para estas medidas de seguridad es el descubrimiento de contenido, que sirve para encontrar dónde se almacenan todos los datos. Una forma de lograrlo es usar las características de descubrimiento de contenido de los productos DLP.

Por ejemplo, una política puede requerir que los números de la tarjeta de crédito del cliente se almacenen solo en los servidores aprobados. Si los datos se detectan en un servidor no autorizado, se pueden cifrar o eliminar, o se puede enviar directamente una advertencia al propietario de los datos, por medio de una notificación personal a su dispositivo en uso.

c) Los datos en uso (DIU) son todos los datos con los que un usuario está interactuando. Los sistemas relacionados con puntos finales se utilizan para proteger los datos en uso y para monitorear los datos a medida que el usuario interactúa con ellos. Por lo general, un agente usa para monitorear los datos mientras se transportan desde un dispositivo o cliente de punto final a través de diferentes canales de salida a dispositivos periféricos. La idea subyacente es que si se intenta enviar datos confidenciales, la posible fuga se detectará de inmediato y será bloqueada antes de que se pueda enviar toda la información.
d) Los datos en movimiento (DIM) son datos que se envían a través de una red. Estos datos pueden enviarse dentro de la red interna de una organización o pueden cruzarse a una red externa (Rendon, 2014).

En términos generales, las soluciones DLP se utilizan para detectar e inspeccionar datos que se envían a través de canales de comunicación a través de una red mediante protocolos conocidos, incluidos correo electrónico, http, mensajes instantáneos e incluso protocolos desconocidos (simplemente inspeccionando el contenido de los paquetes). Si se permite el cifrado o las conexiones cifradas sin la capacidad de descifrar los datos, una solución DLP no podrá detectar fugas de datos en movimiento confidenciales cifrados. En la tabla 1 se muestran las tecnologías asociadas a DLP.

Tabla 1.

Tecnología asociada a DLP

Tipo de tecnología	**Propósito**
Herramientas basadas en puntos finales	Control de las capacidades de los usuarios en sistemas de puntos finales.
Herramientas de monitoreo basadas en la red	Detectar e informar sobre datos sensibles en movimiento
Herramientas de escaneo basada en la red	Escaneo de la red y hosts; para identificar y reportar recursos específicos de datos sensibles desprotegidos.
Herramientas preventivas del perímetro DLP	Detectar datos sensibles que fluyen a través de puntos finales y detener el tráfico que viola las reglas de DLP

Tomado de Torres, 2017

2.6 Privacy Enhancing Technologies (PET)

PET se refiere a sistemas tecnológicos destinados a reducir y, en su caso, suprimir el impacto de las tecnologías de información sobre los derechos de protección de datos e intimidad de los usuarios. (Batalla, 2011)

Históricamente se ha considerado que la inclusión de medidas de seguridad basadas en tecnología suponía automáticamente sacrificar el control o las funcionalidades de una aplicación a cambio de un aumento de privacidad. No obstante, es posible, mediante el uso de PET transformar tecnologías invasivas en tecnologías garantes de la privacidad y por tanto no será necesario renunciar a funcionalidades o seguridad (Ernst & Young's, 2011).

Además, permiten minimizar el uso de datos personales, maximizar la seguridad de la información y dar el control a los individuos sobre la misma. De forma resumida, las protecciones de privacidad que las principales tecnologías disponen se clasifica en las siguientes tres categorías:

a) **Protección de la identidad**
   La cual tiene como objetivo evitar que las verdaderas identidades de los usuarios sean revelados (es decir, quienes son).
b) **Reclusión**
   Intenta evitar que los usuarios sean molestados por contacto o con una solicitud no deseada (por ejemplo, correos electrónicos no deseados).
c) **Control sobre los datos**:
   Permite a los usuarios tener control sobre sus datos, por ejemplo; con respecto a qué datos se pueden recopilar o divulgar, con qué propósito, cómo se utilizarán los datos y con quién o a quién se puede compartir la información (Taal, Le, Leon, Sherer, & Jenson, 2017).

La Comisión Europea afirma que “El uso de los PETs puede ayudar a diseñar Sistemas de Comunicación y servicios de forma que disminuyan la recolección y uso de datos personales y faciliten el cumplimiento de la regulación de protección de datos”. (Comision Europea, 2007)

En general las tecnologías PET se enfocan en:

- Reducir el riesgo de romper principios de privacidad y cumplimiento legal.
- Reducir al mínimo la cantidad de datos que se tienen sobre los individuos.
- Permitir a los individuos mantener siempre la gestión y el control de su información (Hoven & Blaauw, 2014).

Algunos ejemplos de PET son:

- La disociación (anonimización o mantenimiento anónimo) automática de los datos. Los datos deben ser almacenados en un formato que permita identificar al interesado únicamente durante el tiempo necesario para la consecución de las finalidades para las que fueron obtenidas inicialmente. Así, una vez que los usuarios no se encuentren activos, será, por tanto, necesario disociar toda la información.
- El uso de instrumentos de cifrado que impidan el acceso no autorizado a la información transmitida a través de Internet, evitando así el tratamiento no autorizado e ilícito de los datos personales publicados en internet.
- El uso de anuladores de *cookies*, que impiden que el sitio web pueda instalar en los equipos de los usuarios ficheros que, de forma automática y sin que el usuario lo conozca, recopile toda la información estadística y relativa a los accesos que el usuario lleva a cabo durante su navegación.
- La Plataforma de Preferencias de Privacidad (P3P), que permite a los usuarios analizar y comparar las políticas de privacidad de los sitios web que visita, otorgándole un informe sobre la adecuación de éstas a la normativa aplicable.
- Los sistemas de gestión de identidad, que permiten el control por parte de los usuarios de los datos que revelan sobre sí mismos en cada transacción, como los promovidos por el proyecto *Privacy and Identity Management for Europe* (PRIME). (Volpato, 2016, pág. 320)

2.7 Privacy by Design (PbD)

Esta expresión alude a la protección tecnológica de la privacidad desde el mismo momento del diseño de la aplicación, es decir, desde su concepción. Además, PbD se extiende a una "trilogía" de aplicaciones que abarca tres grupos, como son:

- Sistemas de TI.
- Negocio responsable de prácticas.
- Diseño físico e infraestructura en red.

Los principios de privacidad por diseño pueden aplicarse a todo tipo de información personal, pero deben aplicarse con especial énfasis en datos sensibles (Cavoukian, 2011). PbD se establece con base en siete principios que podrían resumirse en los siguientes términos:

a) **Proactivo, no reactivo, preventivo y no remediador.**

   Un sistema basado en este enfoque tiene como finalidad prevenir que ocurran riesgos o infracciones de privacidad. En resumen, previene el problema llegando antes del suceso, no después.

b) **Privacidad como configuración predeterminada.**

   El enfoque hacia la protección de datos debe ser considerado y diseñado para ejecutarse de forma automática. Esto mantendrá la privacidad de los datos intacta y sin necesidad de un ente supervisor.

c) **Privacidad infiltrada en el diseño.**

   La privacidad no es un elemento complementario del proceso de diseño y construcción de los sistemas informáticos, sino la raíz y esencia de los mismos, constituyendo su parte integral sin reducir su funcionalidad.

d) **Funcionalidad completa.**

   En este sistema, rige el principio general de ‘todos ganan’ y se huye a la máxima ‘si alguien gana otro pierde’, dado que su aceptación supondría aceptar la posibilidad de una reducción en el grado de protección de datos a favor de otros elementos sustanciales del sistema como su estabilidad o su seguridad.

e) **Protección extremo a extremo en el ciclo de vida.**

   Los sistemas de recogida y tratamiento de datos asegurarán unos niveles máximos de protección de la información tanto en su recogida como en las posteriores fases de las que se componga el ciclo de vida

de tales datos en los citados sistemas. De este modo, los datos se recogerán, tratarán, y finalmente destruirá, estableciéndose así una administración segura de la información desde un extremo a otro.

f) Visibilidad y transparencia

La explotación de los sistemas técnicos que vayan a utilizarse para el tratamiento de datos personales deberán estar estructurados y funcionar conforme a su diseño original, garante de unos niveles óptimos de protección de tal información. Así, sus componentes y operaciones deberán ser transparentes para todos sus usuarios, de modo que éstos tengan una imagen fiel en todo momento del status de cumplimiento de los niveles de protección de datos personales.

g) Respeto por la privacidad del usuario

El usuario es el elemento prioritario principal. De este modo, los intereses de tales usuarios deberán configurar los sistemas, implicando el desarrollo de elementos en los mismos como, por ejemplo, configuraciones predefinidas de privacidad alta, sistemas adecuados de notificaciones así como establecer medios de opciones para los perfiles de usuario de fácil gestión. (Cavoukian, 2011, pág. 2)

En definitiva, una red garante de la privacidad y que vaya de la mano con filosofía PbD debe asumir como principio base que el usuario es dueño de su información, y que por tanto, no sólo debe mantener sino reforzar sus derechos y privacidad. De hecho, el Supervisor Europeo de Protección de Datos (del inglés, *European Data Protection Supervisor*, EDSP) recomienda el uso del PbD y sugiere la adopción de esquemas de certificación de la privacidad y de los datos personales (Volpato, 2016, pág. 325).

Además, PbD requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como una mayor robustez, notificación apropiada, y facultando opciones amigables para el usuario. Por otro lado, esta técnica viene dada por 4 fases, establecidas de la siguiente manera:

Primera fase: Validación

a) **Preanonimización de los microdatos**

La privacidad comienza antes incluso de empezar a almacenar la información en las bases de datos. El proceso de anonimización se inicia con la caracterización de aquellas variables (directas o indirectas) a partir de las cuales se puede lograr la identificación del usuarios, a este proceso se le conoce como preanonimización de los microdatos (Baladán, Betarte, Blanco, Montaña, & Muracciole, 2016)

Una vez que se ha realizado una categorización de las variables se establecen los criterios de protección necesarios para garantizar la privacidad de las personas, tratando de minimizar la cantidad de información personal que vaya a ser utilizada durante el proceso de anonimización. Por tanto, en esta primera fase del proceso se determina, según las regulaciones específicas de cada país; qué tipo de datos se puede almacenar y durante cuánto tiempo. (Baladán, Betarte, Blanco, Montaña, & Muracciole, 2016)

b) **Eliminación/reducción de variables**

Posteriormente se busca disminuir al mínimo o eliminar el número de variables a partir de las cuales se puede lograr la identificación del usuario, en esta fase se permite solo al personal necesario poder acceder a la información de carácter confidencial.

El objetivo de estos procesos es someter a los datos anonimizados a un proceso de agregación. Este proceso sirve para evitar que se pueda identificar a individuos concretos. Por ello se agrupan por perfiles, por ejemplo, creando rangos geográficos o temporales con el objeto de evitar que los datos puedan facilitar la identificación de individuos concretos. (Baladán, Betarte, Blanco, Montaña, & Muracciole, 2016)

c) **Anonimización de los procesos y datos locales**

Tras estas dos fases de “preparación” de los datos, llega el momento de aplicar técnicas y estrategias de anonimización de los procesos y anonimización de datos locales:

- Preferencias de privacidad.
- Estrategias de cifrado y enmascaramiento de la identidad.

Las preferencias de privacidad tienen que ver con la protección en la fase de generación de datos. La generación de datos puede ser activa, cuando el propietario de los datos los facilita a un tercero, o pasiva, cuando los datos se generan por su actividad *online* (por ejemplo, navegar por internet o participar en una red social). Para evitar que esto ocurra sin que el usuario sea consciente de ello, la PbD especifica que las opciones por defecto sean lo más respetuosas posible con la privacidad del usuario y que sea el propio usuario, el que tenga que tomar la iniciativa de desactivar o rebajar el nivel de protección cuando así lo desee (Narayanan & Shmatikov, 2008).

En estos casos, hay dos estrategias principales de protección de la privacidad, por un lado, las de restricción de acceso, como las extensiones *anti-tracking*, bloqueadoras de anuncios o *scripts*, y herramientas de cifrado, del otro lado, las herramientas de cifrado de datos y enmascaramiento de la identidad que introducen pequeñas distorsiones ("ruido") en los datos y los modifican de forma que no sea posible identificar a un usuario individual (Narayanan & Shmatikov, 2008).

Segunda Fase: Validación de procesos *Map Reduce*

Esta fase permite aplicar las especificaciones de privacidad relativas a cómo reaccionan los datos al hacer una consulta, y añadir restricciones a la compartición de datos entre distintos procesos (Baladán, Betarte, Blanco, Montaña, & Muracciole, 2016).

Tercera fase: Validación del proceso *Extract, Transform and Load* (ETL)

Los procesos ETL son los responsables de la extracción de los datos a partir de las diversas fuentes de datos heterogéneas, de la transformación de estos (conversión, limpieza, etc.), y de su carga en el almacén de datos, son un

término estándar que se utiliza para referirse al movimiento y transformación de datos. (Muñoz, Pardillo, Mazón, & Trujillo, 2016)

La seguridad de los datos, en cuanto al control de accesos, se puede implementar a nivel de fichero, de base de datos, de comunicaciones y cifrado de aplicaciones. Aunque se trabaje con datos anonimizados, y los resultados se ofrezcan siempre de forma agregada, en muy importante, mantener un control estricto del acceso a la información a lo largo de todo el proceso (desde las fases de ingesta de dato a las fases finales). Es fundamental asegurarse de que la incorporación de nuevos conjuntos de datos no implique riesgos inadvertidos de des-anonimización de los datos originales.

Cuarta fase: Reportes

En esta fase, la comprobación del cumplimiento de los términos de privacidad tiene que ver con asegurar que se respeta la finalidad para la cual se han tomado los datos, comprobando que en los informes no aparezca información sensible. Es decir, asegurarse de que no se puedan recopilar más datos de los necesarios para los fines previstos, explícitos y legítimos (Baladán, Betarte, Blanco, Montaña, & Muracciole, 2016).

También es fundamental que las políticas de publicación de resultados se apliquen de forma consistente y correcta. Para ello se aplica un conjunto de técnicas que garantizan que no es posible revertir el proceso de anonimización de los resultados obtenidos.

2.8 Bloqueo de puertos

Las nuevas empresas que se relacionan con las Tecnologías de la Información y Comunicación hacen uso de diversas técnicas y herramientas de redes para el intercambio de datos como son:

- La transferencia de archivos vía ftp.

- La transferencia de datos e información a través de Internet por el servicio de red http.
- Conexiones remotas a máquinas y servidores a través de telnet (Capo, 2015).

Se pueden considerar que, los tres anteriores protocolos, son de mayor riesgo a la hora de transmitir información y para controlar su riesgo especialmente en los puertos, éstos son gestionados por los diversos sistemas que operan dentro de una red. El control de puertos abiertos en entorno web es un elemento extremadamente peligroso, debido a la facilidad de establecer un enlace; esto puede provocar que se ejecute un programa en el cliente e infecte la máquina, dejándola abierta para otros ataques o para que colabore en la ejecución de otros ataques. (Taluja, Kumar, & Lal, 2012)

El punto más vulnerable es la constante transmisión por el puerto http (8080) de internet que representa siempre una puerta abierta a los intrusos. Ante esto equivale la política del bloqueo de algunos servicios de red de la maquina origen, permitiendo sólo el control de aquellos que son absolutamente necesarios. (Taluja, Kumar, & Lal, 2012)

También, se hace necesario que protocolos como Telnet y el Protocolo de Transferencia de Archivos (FTP), aparte de utilizar su propias técnicas de transporte seguro, puedan decodificar los datos de salida y entrada a la redes con formatos seguros como el *American Standard Code for Information Interchange* (ASCII) o binario. Adicionalmente como medida de seguridad se deben proteger los canales para tramitar el intercambio, envío o consulta de datos personales, el cual fundamentalmente se llevan a cabo mediante el Protocolo de Transferencia de Hipertexto (HTTP). (Simpson & Foltz, 2016)

Mediante el protocolo HTTP se cifra la información en los sistemas de telecomunicaciones; en la actualidad los dos protocolos más utilizados en la industria consiste en Seguridad de la Capa de Transporte (del inglés, *Transport*

Layer Security, TLS) y Capa de Puertos Seguros (del inglés, *Secure Sockets Layer,* SSL).

Tanto TLS y SSL aplican la criptografía asimétrica de enclave pública, para autenticar al servidor, para el uso de firmas digitales; sin que sea obligatoria la autenticación del cliente, sin embargo las criptografía para las transmisiones de información se realiza mediante clave simétrica o privada. (Capo, 2015)

2.9 Certificado digital

Este tipo de certificado es un documento electrónico que se utiliza para identificar a una persona, un servidor, una empresa o alguna otra entidad, y para asociar esa identidad con una clave pública. Por ejemplo, al igual que una licencia de automóvil, una cedula de identidad, un pasaporte, una papeleta de votación u otras identificaciones personales de uso común, un certificado digital proporciona una prueba generalmente reconocida de la identidad de una persona. Por lo general, los certificados utilizan criptografía de clave pública para solucionar el problema de la suplantación. (O'Brien & Weir, 2017)

Las autoridades de certificación (CA) son entidades encargadas de validar las miles de identidades y de emitir los certificados. En general, antes de emitir un certificado, la CA debe utilizar sus procedimientos de verificación publicados para ese tipo de certificado para garantizar que la entidad que solicita un certificado sea, de hecho, quien dice ser. (O'Brien & Weir, 2017)

En relación a la navegación por internet y el uso de correo electrónico, es importante identificar que este certificado esté presente en las páginas web, garantizando así su calidad y fiabilidad. Por lo general la URL a de comenzar por https://, en lugar de http, y aparecer un icono con un candado cerrado. Además, este certificado digital confirma la autenticidad de la página y con ello, se extremarán las precauciones por si se va a realizar alguna compra en línea o un registro de datos, precautelando la confidencialidad de la información a

través de internet. Por ejemplo, según la Ley 59/2003 de firma electrónica promulgada y valida únicamente en España, existen otros tipos de certificados:

a) Certificados corporativos reconocidos: son certificados cuyo suscriptor es una corporación (ya sea una empresa, una organización, un gremio profesional, etc.).
   Ejemplo: Certificado de persona natural corporativa; son certificados reconocidos para personas físicas que identifican al suscriptor como vinculado a una determinada organización, ya sea como empleado, asociado, colaborador, cliente o proveedor.
b) Certificados reconocidos para las administraciones públicas: son certificados electrónicos emitidos sobre el acceso electrónico de los ciudadanos a los servicios públicos.
   Ejemplo: Certificado de sello de administración, organismo o entidad de gestión pública. Son certificados para dispositivos informáticos, programas o aplicaciones dedicados para firmar en nombre del organismo en los sistemas de firma electrónica para procedimientos administrativos automáticos (Berrocal, 2016) .

3. CAPÍTULO III. MARCO REGULATORIO PARA LA PROTECCIÓN DE DATOS

3.1. Protección de los datos personales sensibles

Los datos personales sensibles, deben ser protegidos por las leyes y el Estado, así como por los consumidores o usuarios de los sistemas de información. El principal uso de los datos informáticos se asemeja a un instrumento de comercialización, a través del cual las empresas utilizan esta información para la venta de sus productos sin que exista un consentimiento expreso por parte del titular.

El origen de la protección de datos es europeo y proviene del reconocimiento del derecho a la intimidad personal y familiar. El primer antecedente normativo,

se encuentra en el artículo 12 de la Declaración Universal de los Derechos del Hombre, adoptada en París por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948, que establece en líneas generales que; todo individuo debe ser protegido con respecto a intrusiones arbitrarias en ningún aspecto relacionado con su vida privada o familiar, que puedan ocasionar ataques en su contra o de su reputación, y concluye que esté debe ser un derecho ciudadano. (Pulido, 2013, pág. 87)

Durante el año 1967, el Consejo de Europa creó una Comisión que tenía como objetivo, estudiar las tecnologías de la información y el efecto de estas sobre el derecho de las personas, el resultado de dicha Comisión se recogió en la Resolución 509 de la Asamblea del Consejo de Europa sobre los derechos humanos y los nuevos logros científicos y técnicos. Dicha Resolución es considerada el inicio de la regulación para la protección de los datos personales.

El 8 de mayo de 1979, el Parlamento Europeo aprobó una Resolución sobre tutela de derechos del individuo frente al desarrollo de la informática. También en este periodo, el derecho a la protección de datos comienza a recogerse explícitamente en los textos constitucionales. A partir de 1980, se sitúa una etapa marcada por varios acontecimientos importantes:

- Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre la circulación internacional de datos personales para la protección de la intimidad, en septiembre de 1980.
- El 28 de enero de 1981, el Consejo de Europa firma el Convenio 108 relacionado al uso automatizado de los datos carácter personal.
- Resolución de 14 de enero de 1990 de la Asamblea General de las Naciones Unidas, relativa a los principios rectores para la reglamentación de los ficheros computarizados de datos personales.
- La Directiva de Protección de Datos (95/46/CE), del Parlamento Europeo y del Consejo, implantó que la realización de transferencias

internacionales de datos personales, con destino a Estados no miembros de la Unión Europea (UE), queden limitadas a que dichos Estados garanticen un mismo nivel de protección, lo que en la práctica ha derivado en que las normativas de aplicación en los diferentes países hayan ido uniformizándose.

3.2. Tratamiento de los datos personales

El tratamiento de los datos personales ha tenido su trascendencia, y en parte es gracias a la utilización masiva de la informática. La vida privada del individuo está marcada por un sinfín de facetas, por ello si se trata de manera conjunta por medios informáticos puede llegar a construir un perfil donde el mismo titular desconoce.

Es por esa razón que la inmensa transformación tecnológica, ha permitido reaccionar y proteger a uno de los derechos fundamentales que es la protección de datos de carácter personal. El principio para el tratamiento de los datos personales se puede manifestar en los siguientes aspectos:

Consentimiento

Este principio fundamental, se refiere a que tanto el titular decide, quien, cuando, como y para que se manejan sus datos.

Información

Los usuarios deben tener conocimiento de quién, cómo y para qué se va a emplear su información, así como poder ejercitar, en su caso, los derechos que la Ley le reconoce.

Rectificación

Este principio permite que los titulares de los datos soliciten la modificación, en caso de que los datos sean inexactos, y que hayan dejado de ser pertinentes y

necesarios para la finalidad para la cual hubiere sido registrada y, posterior pedir su cancelación.

Uso

Los datos personales se pueden utilizar y manejar en el momento que el titular así lo desee, es decir la información está al alcance del titular.

3.3. Principios de la ley de protección de datos

Los principios establecidos por la doctrina, en materia de protección de datos de carácter personal, tienen la intención de determinar conceptualmente el modo más eficaz de proteger la intimidad de las personas frente a la evolución de las tecnologías de la información y de las comunicaciones. Se busca proteger a la persona, a los efectos de que ella salvaguarde su libertad, ejerciendo el dominio y el poder de decisión sobre sus datos personales.

3.4. Regulación internacional de protección de datos

Las normas sobre protección de datos son responsabilidad de los estados o gobiernos, cada país tiene la libertad de desarrollar las leyes según sus principios y necesidades; a continuación, se muestran los principales desarrollos que se han presentado en esta materia:

- **Organización de Naciones Unidas (ONU)**
  La ONU adopta como criterio primordial la Declaración Universal de Derechos Humanos en la cual en su art. 12 establece que todo individuo tiene derecho al resguardo de sus datos personales.
- **Unión Europea**
  El Convenio de Estrasburgo también conocido como Convenio 108 fue el primer acuerdo de carácter internacional firmado por Alemania, Dinamarca, Francia, Luxemburgo y Austria en el año 1981,

posteriormente se creó la Directiva 95/46/CE la cual regula lo referido a las comunicaciones y el tratamiento de datos personales.

- **Alemania**

  Firma su primer convenio para la protección de datos personales en 1970 y en el año 1977 se aprueba la Ley Federal *Bundesdatenschutzgesetz* el cual establece que queda terminantemente prohibido la transferencia de información de tipo personal sin la previa autorización del dueño del dato.

- **Suecia**

  Este país fue pionero en la propuesta y promulgación de leyes relacionadas a la protección de datos, su primera normativa fue publicada en el año de 1973, la cual prevé un órgano de control, encargado de velar por su aplicación, recibir las reclamaciones de los afectados y dotado de potestad reglamentaria, cuyo ejercicio ha garantizado la perdurabilidad normativa.

- **España**

  España emitió la ley para la Protección de Datos en el año 1999, la cual ha sido utilizada por Latinoamérica y es un referente del estándar europeo, en el año 2018 exigirá el consentimiento del titular de cualquier dato para que un tercero pueda utilizarlos, así como el derecho al olvido en Internet.

- **Rusia**

  Este país desarrollo una importante normativa para la regulación de los datos personales, la cual se firmó en el año 2006, en la actualidad este país ha realizado varios cambios entre los que se destacan, el que obliga a las compañías nacionales y extranjeras a guardar la información privada de los internautas rusos en servidores ubicados en el territorio del país.

- **Estados Unidos de Norteamérica**

  Su normativa fue promulgada en el año 1974 y tiene su origen en *Privacy Act.*, la cual se considera ambigua y destaca que no existen

autoridades que vigilen el cumplimiento de protección de datos además que existe poca jurisprudencia al respecto.

- **Latinoamérica**

  Las normativas desarrolladas en Latinoamérica se basan en el modelo europeo, fueron promulgadas por la necesidad imperante de controlar las transmisiones de información y debido a la detección de numerosas fallas en torno a la seguridad en las telecomunicaciones. En Chile se firmó en el año 1999; en Brasil fue en el año 1994, Uruguay en el año 2008, Paraguay, Argentina en el año 2000 y en Perú en 2011.

- **Perú**

  Este país presenta la Ley con desarrollo más reciente, la cual se firmó en el año 2011, que refleja las disposiciones de la UE a pesar de no haber tenido ninguna regulación previa en la materia.

- **México**

  En el año 2010, se firmó la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la cual es la base de un sistema de privacidad integral que rige el tratamiento de datos personales, incluyendo su obtención, uso, transferencia y almacenamiento. En la Figura 1, se muestra el avance de la ley de protección de datos en el mundo.

Figura 1. Protección de datos personales en el mundo.
Tomado de Alarcón, 2018.

3.5. Marco jurídico actual en Ecuador

A continuación se analizará las normas jurídicas sobre protección de datos que se dispone actualmente en Ecuador.

3.5.1. Constitución de la República del Ecuador

La Constitución instituye la protección de datos personales en el art. 66, numeral 19:

> *"*El derecho a la protección de datos de 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 o información requerirán la autorización del titular o el mandato de la ley". (Ecuador, 2008)

3.5.2. Ley de comercio electrónico, firmas electrónicas y mensajes

La Corporación Ecuatoriana de Comercio Electrónico (CORPECE) es una institución multiactorial y multidisciplinaria que promueve el desarrollo del comercio electrónico y la economía digital y se encarga del área de estudios, creación de programas y proyectos para impulsar el uso, desarrollo y aplicación de TIC's en el país (CORPECE, 2016).

El 17 de abril de 2002, creó y promulgó la Ley No. 67. RO/ Sup 557, que lleva por título Ley de comercio electrónica, firmas y mensajes de datos. Entre los aspectos relevantes de la presente ley se establece lo siguiente:

- Precautelar los derechos de los usuarios que hacen negocios en internet desarrollando normativas para la publicidad en línea, fortaleciendo el derecho a la privacidad de los usuarios y otros temas de protección al consumidor. Todo ello, se encuentra orientado a un medio completamente nuevo en el país, en el cual es necesario innovar para estar acordes a la tecnología y a los nuevos modelos de negocios.
- Modificar el código penal para incluir sanciones por los denominados delitos informáticos que comprenden el fraude electrónico, la intercepción de mensajes de datos, el ingreso no autorizado a información en sitios privados.
- Se establece la figura del Certificado Digital, que garantiza las transacciones en la red, identificando de forma única a un proveedor de servicios o bienes. Además, al ser un entorno donde no se ve físicamente al vendedor, por tanto, es necesario contar con un método para identificarlo y asegurar su capacidad.
- Se establece que las firmas electrónicas son los datos en forma electrónica o un conjunto de algoritmos matemáticos complejos, que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y

> reconoce la información contenida en el mensaje de datos. Se consideren con igual validez jurídica que las firmas manuscritas (Congreso Nacional, 2002).

Además, esta ley provee la única definición sobre datos personales existente en la legislación ecuatoriana: “Datos personales: son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley”. (Congreso Nacional del Ecuador, 2002) Y como puntos a destacar, la Ley de Comercio establece lo siguiente:

> “Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros”. (Congreso Nacional, 2002)

Lo que implica que se requiere el consentimiento del titular de los datos para la elaboración, transferencia o utilización de bases de datos. Y en aquellos casos que la finalidad de dicha información no esté justificada y sin el consentimiento, será considerado una infracción grave que requerirá alguna sanción. También, la Ley hace hincapié en que la recolección responderá a los derechos constitucionales de privacidad, intimidad y confidencialidad.

> “Art. 32.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley”. (Congreso Nacional, 2002)

El Reglamento a la Ley de Comercio Electrónico por su parte en el Art.21, determina que las entidades que presten servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de

prestación de dicho servicio. De tal forma que, el ente que maneja los datos tiene la obligación de informar a los usuarios sobre los mecanismos de seguridad utilizados en este proceso, en caso de existir.

3.5.3. Ley del sistema nacional del registro de datos públicos

Según esta ley, los datos públicos son aquellos que constan en los registros de datos públicos, sin hacer una diferencia con datos personales protegidos:

> "Art. 13.- De los registros de datos públicos. - Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes". (Ecuador, 2008)

3.5.4. Código orgánico integral penal

Este código tipifica el delito de violación a la intimidad art. 18:

> "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años". (Ecuador, 2014)

3.5.5. Habeas Data

Esta frase significa literalmente, "traer los datos", es decir, traer los datos personales del actor, a fin de que éste pueda conocerlos y resolver lo

pertinente acerca de ellos. La finalidad es la protección de los datos personales ante el llamado poder informático (Caicedo, 2014).

La figura del *habeas data* es, de conformidad con la normativa constitucional y legal aplicable a la fecha en el Ecuador, una acción de garantía, de rango constitucional, la misma que protege determinados derechos constitucionales.

El habeas data es una garantía Constitucional cuya naturaleza es ser acción, esta genera un proceso constitucional, el mismo que terminara con una resolución, y que mediante determinadas condiciones puede ser objeto de ciertos recursos, entre ellos el de apelación ante el superior jerárquico (Briones, 2017).

Tradicionalmente, se afirma que el *habeas data* protege el derecho a la intimidad, el cual, como sabemos, no solo es personal sino hasta familiar. Pero, además de la intimidad, también pueden ser afectados, mediante informaciones incorrectas, el honor, la buena reputación y la imagen de las personas.

Hay que aclarar que algunos derechos como el respeto al honor, a la buena imagen, no necesariamente es vinculado con el derecho a la intimidad personal; es decir, se puede afectar al honor, sin que necesariamente la materia de la ofensa se refiera a la intimidad de la persona.

3.5.6. Código orgánico general de procesos (COGEP)

Una de las reformas legales de mayor importancia de la última década en el Ecuador es la relacionada con la promulgación del COGEP. La finalidad de esta normativa es determinar una forma de sustanciación común de distintos tipos de procesos judiciales de diversas materias, los cuales antes se hallaban dispersos y presentaban ciertas formalidades innecesarias que lo tornaban

complejo, y sobre todo que no acreditaban las garantías procesales suficientes como la Constitución de la República lo exige en la actualidad.

El COGEP, contempla de manera indirecta, el derecho a la protección de datos personales, en su artículo 7, que establece lo siguiente:

> Art 7.- Principio de intimidad. Las y los juzgadores garantizarán que los datos personales de las partes procesales se destinen únicamente a la sustanciación del proceso y se registren o divulguen con el consentimiento libre, previo y expreso de su titular, salvo que el ordenamiento jurídico les imponga la obligación de incorporar dicha información con el objeto de cumplir una norma constitucionalmente legítima". (Republica de Ecuador, 2015)

Según lo establecido en el párrafo anterior, esta ley instituye la presencia del principio de intimidad para la protección de los datos personales correspondientes a los implicados en un querella judicial, sin embargo no presenta una diferencia entre lo que corresponde a datos personales de los datos íntimos.

3.5.7. Ley Orgánica de Telecomunicaciones (LOT)

El 21 de junio del 2013, la Asamblea Nacional aprueba la Ley Orgánica de Comunicación; la misma que se publica en el Registro Oficial 22, Tercer Suplemento del 25 de junio del mismo año. Esta Ley contiene 119 artículos distribuidos en seis títulos. El Título II contiene dos capítulos, al igual que el Título III; el Título V contiene ocho secciones. Constan también 24 disposiciones transitorias, 2 disposiciones derogatorias, 6 disposiciones reformatorias y una disposición final.

En esta ley, el *CAPÍTULO* I "condiciones generales comunes tanto para contratos de adhesión como para contratos negociados" establece en el Art. 4.- Condiciones generales que deben cumplir los prestadores de servicios.

Privacidad y protección de datos.- Los prestadores de servicios de telecomunicaciones y/o servicios de radiodifusión por suscripción deben garantizar la privacidad y protección de los datos personales entregados por los abonados, suscriptores o clientes, para lo cual implementarán mecanismos necesarios para precautelar la seguridad de dicha información, incluyendo el secreto e inviolabilidad del contenido de sus comunicaciones, con las excepciones previstas en la Ley. (Asamblea Nacional de Ecuador, 2015)

Lo que implica que el estado ecuatoriano reconoce que los ciudadanos tienen derecho a la privacidad y la protección de nuestros datos personales por parte del prestador con el cual se contrate algún servicio.

Los prestadores de servicio de telecomunicaciones, siempre manejan los datos personales y deben cumplir ciertas obligaciones ; en la misma ley antes mencionada en su artículo 78, se establece las garantías que se dan frente a los datos personales entre las cuales están la de garantizar la aplicación de una política efectiva de protección de datos personales, la información al usuario respecto a cualquier tipo de sesión o tratamiento de sus datos personales; además que el prestador debe contar con un personal autorizado para que realice el tratamiento de los datos personales.

Claramente, esta ley no tiene normas explicitas acerca de la protección jurídica de los datos personales; por lo que hay que especificar que lo que se precautela en esta norma es la privacidad de las personas que brindan su información para diferentes propósitos dentro de los contenidos de los servicios de telecomunicaciones.

3.5.8. Reglamento general de la ley orgánica de telecomunicaciones

En esta ley se establecen los avales sobre las actividades que realizan los entes prestadores de servicios de telecomunicaciones para garantizar la

seguridad sobre el uso y disposición de datos personales, además define la imponencia de la protección de datos en los servicios informáticos.

En el Reglamento General a la Ley Orgánica de Telecomunicaciones en el TITULO XV. Secreto de la Comunicación y Protección de datos, establece:

> "Art. 120.- Garantía de protección de datos personales.- Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, esto es, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la LOT, su Reglamento General y las regulaciones emitidas por la ARCOTEL para el efecto. La violación de esta garantía dará lugar a la imposición de las sanciones previstas en el ordenamiento jurídico.
>
> Art. 121.- Uso comercial. - Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora; salvo autorización y consentimiento expreso del usuario." (Presidente Constitucional de la República, 2016)

3.6. Propuesta de ley de protección de datos Ecuador

La Ley Orgánica de la Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales, la cual tiene como finalidad primordial la protección de datos personales que se encuentren en bases privadas o públicas; regular el uso de los mismos para proveer de privacidad a la ciudadanía a través de la emisión de la presente ley, este proyecto está conformado por una disposición transitoria, reformatoria y veintiocho artículos.

El proyecto de Ley asume entre sus principales objetivos; otorgar a los ciudadanos las potestades sobre sus datos personales ante terceros, que por uno u otro motivo tengan acceso a la información personal, en función al criterio universal de privacidad e intimidad del ser humano; y posteriormente regular cualquier tipo de tratamiento sobre los datos personales que reposan en base de datos. En función de lo establecido en la presente ley, se identificaron los principales aspectos técnicos regulatorios:

En Ley Orgánica de la Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales se establece definiciones tales como dato persona, responsables, riesgos, sanciones etc, y hace énfasis en la diferencia existente entre un dato íntimo y un dato de carácter personal.

También, decreta los derechos de los ciudadanos sobre el uso de los datos personales, definiendo los conocidos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) correspondiente a los datos personales. Finalmente instituye sanciones a los entes responsables del tratamiento de datos, estableciendo ciertas obligaciones legales, entre las que se mencionan la autorización previa del titular, y asistir a los ciudadanos en la aplicación de los derechos ARCO, entre otras.

Sin embargo, la presente ley contiene debilidades en lo que corresponde en primer término a las sanciones administrativas, en las cuales no se establece el procedimiento judicial en caso de incumplimiento por parte de responsable del tratamiento de datos y en segundo término no indica cuales son los mecanismos técnicos o tecnologías que deben incorporar a los sistemas informáticos a fin de optimizar y salvaguardar la información que resguarda la presente ley.

Las principales debilidades en el ambiente técnico de los sistemas de comunicación, en la propuesta de Ley para la protección de datos en Ecuador, está relacionada a los siguientes puntos:

a) Responsable del tratamiento de datos, donde se establece que la responsabilidad es del administrador; siendo ésta una definición incompleta. El hecho es que existe una confusión entre las funciones del encargado y el responsable del tratamiento de datos. Se establece que el responsable de una base de datos puede ser responsable y/o encargado del tratamiento de datos. Por un lado, será responsable si ha recibido la autorización de determinar los medios y fines del tratamiento por parte del titular de los datos personales. Y por el otro lado, será el encargado si realiza el tratamiento de datos por cuenta del responsable.
b) Con relación a la regulación en torno al tema de la seguridad, este proyecto de ley no regula la protección de manera específica. Es decir, no contempla la regulación de la pseudonimización, ni el cifrado, ni la aplicación de estándares de seguridad. La técnica de pseudonimización pretende simplificar el hecho de conocer la identidad de una persona, con el fin de precautelar sus datos personales. Su diferencia con el anonimato radica en que la anonimidad supone la imposibilidad de conocer la información de la persona (Álvarez, 2017).

4. CAPÍTULO IV. RIESGOS ENTRE LOS SISTEMAS DE TELECOMUNICACIONES Y LA PROTECCIÓN DE DATOS

El tratamiento de datos personales se ha convertido en una práctica habitual en nuestros días y su comercialización se enfoca hacia un negocio que mueve un inmenso caudal de dinero.

Las empresas tienen sumo interés en conocer y manejar los gustos, preferencias, hábitos de consumo de la población, dado que ello les permitirá orientar su producción a las necesidades de consumo, desarrollar publicidad a medida de los consumidores y optimizar el uso de sus recursos en producir aquello que más ventas les garantice. En definitiva, lo que buscan es liderar el mercado con un fin netamente económico, sin importarles cómo llegan a ese objetivo. Es decir, que no las detiene saber que sus prácticas implican

intromisiones en la privacidad de los consumidores porque su foco se ubica en incrementar sus ganancias sea como sea.

Además de las empresas fabricantes de productos, existen otros actores sociales que también tienen interés en conocer y manejar nuestros datos para ventas, publicidad, investigación e incluso usos ilegales, en general las empresas desean nuestra información para múltiples fines como:

El marketing directo: existen empresas de marketing que se dedican a elaborar publicidad a medida de los clientes, de acuerdo a sus gustos e intereses, logrando con ello mayor eficacia. Es habitual que nos llegue a nuestro correo electrónico ofrecimientos de todo tipo, vinculado a nuestras necesidades de consumo del momento.

Elaboración de estadísticas y control: también el Estado puede tener interés en recabar nuestros datos, en principio, con fines de control por ejemplo respecto de la propagación de alguna enfermedad como la Hepatitis B que le permita evaluar la necesidad o no de campañas sanitarias de vacunación y prevención.

Sin embargo, el hecho de que el Estado y sus agentes dispongan de demasiada información personal de la población puede implicar un grave riesgo, sobre todo cuando se producen quiebres institucionales. Hay muchos ejemplos en la historia que evidencian que cuando los gobiernos tienen un carácter de totalitario, los datos personales se utilizan con fines persecutorios y discriminatorios.

Exclusión de cobertura médica: las empresas prepago suelen recurrir a los rastreos de navegación de los usuarios en la web a fin de indagar el posible padecimiento de alguna enfermedad en sus clientes que pudiera ocasionarle grandes erogaciones, por ejemplo: enfermedades como sida, cáncer o tal vez el consumo de alguna droga o medicamentos costosos. O bien suelen recurrir

a bases de datos para conocer datos genéticos y a partir de allí evaluar el riesgo de cada cliente.

Exclusión de asegurados: iguales limitaciones se aplican a los asegurados que quedan fuera del sistema de seguros, ya sea de vida, de retiro, o la cobertura de siniestro de otra índole, etcétera. En base a información sobre antecedentes de clientes, las empresas aseguradoras de diferentes activos o incluso los seguros sobre vida de clientes basan sus estimaciones y decisiones sobre información personal obtenida de forma irregular a través de la web.

Determinación del perfil de futuros empleados: en oportunidades se han formado bases de datos de personas que no pueden acceder a un trabajo, debido a incidentes o en función de su desempeño previo, esta información es adquirida a través de medios digitales e incluso en algunas oportunidades parten de la opinión de usuarios sin verificación previa, las empresas desean conocer a los individuos en diferentes aspectos de su vida, a fin de realizar contrataciones más eficaces.

Fines delictivos: las organizaciones criminales suelen hacer un estudio de sus posibles víctimas antes de actuar, por ello nuestros datos pueden serle de gran utilidad (Gellert, 2015).

La agencia española de protección de datos (AEPD), establece así mismo un conjunto de riesgos relacionados directamente con la información personal que se maneja en internet tanto desde la persona titular de la información, como las responsabilidades de terceros que incurran en delitos relacionados con la manipulación y uso de información personal no autorizada (AEDP, 2014).

Entre los riesgos del uso de información personal considera el principal delito el descubrimiento, revelación de secretos e integridad moral; el cual ocurre cuando terceras personas acceden, sin autorización, a información de otras personas o la difunden a sabiendas de que ha sido obtenida de manera ilícita,

además de estar vulnerando la intimidad, se comete un delito de descubrimiento y revelación de secreto.

También, se pueden producir, como consecuencia del acceso a información confidencial, diferentes acciones como amenazas, coacciones, acoso así como calumnias e injurias, violencia de género, libertad e indemnidad sexual, suplantación de identidad, odio. Uno de los riesgos más comunes relacionados al uso de información personal se refiere a las estafas y daños informáticos; la AEDP establece que una de las modalidades de estafas más comunes en la red es el *pishing.*

Este tipo de ataque se puede definir como el intento de obtener fraudulentamente de los usuarios de Internet sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc., para posteriormente usarlos para sustraer dinero de sus cuentas, ordenando transferencias o para realizar compras o solicitar, por ejemplo, créditos en su nombre. Del mismo modo, en el caso de la privacidad de los datos, las amenazas son principalmente de tres tipos:
Acceso ilegítimo a los datos: está relacionado con la confidencialidad, y aquellos casos donde las personas acceden a información sobre la cual no tienen permiso.

Modificación no autorizada de los datos: está relacionado con la integridad, es decir, cuando los datos con los que se trabaja tienen riesgo o han sido dañados o corrompidos; modificaciones sobre los datos sobre las que no se tiene conocimiento o no han sido solicitadas o aprobadas.

Eliminación de los datos: está relacionado con la disponibilidad; son aquellos casos en los que se pierden o desaparecen datos (Safianu, Twum, & Hayfron, 2016).

4.1. Aspectos técnicos en la protección de datos personales

Una de las mejores opciones con las que cuenta actualmente el mundo de la protección de datos personales frente al advenimiento de la convergencia tecnológica y el internet, puede ser encontrada en las soluciones técnicas adoptadas tanto en el nivel nacional como el internacional, estas soluciones se deben a los procesos de estandarización coordinados por entes como el Grupo de Trabajo de Ingeniería de Internet (IETF), la Organización Internacional para la Estandarización, (ISO), la Unión Internacional de las Telecomunicaciones (ITU) y otros. Entre las que se mencionan:

4.1.1. Grupo de trabajo de Ingeniería de Internet (del inglés, *Internet Engineering Task Force, IETF)*

IETF es uno de los entes internacionales más relevantes en la administración técnica del internet. Relacionada directamente con la Sociedad del Internet y otros entes de gobernanza por múltiples interesados, la IETF ha sido conocida por importantes contribuciones a lo largo de la historia del internet (Peterson, Tschofenig, & Aboba, 2017).

4.1.2. Estándares de la Organización Internacional para la Estandarización (ISO) de la serie 27000

La serie ISO/EIC 27000 corresponde a un conjunto de estándares desarrollados por la ISO y la Comisión Electrotécnica Internacional (IEC), enfocados fundamentalmente al área de la gestión de la seguridad de la información. Estas normas componen un marco de referencia metódico, documentado y basado en objetivos claros, que pueden ser seguidos por toda organización (Hoven & Blaauw, 2014).

4.1.3. Protocolos de comunicación

En el ámbito de las tecnologías de la información, se llama protocolo a un conjunto especial de reglas (establecidas como parte de un estándar abierto internacional o de manera privada como estándares creados por las diversas industrias o empresas) que son utilizadas por los puntos de una red en sus comunicaciones.

Compuestas fundamentalmente por disposiciones relevantes al cifrado de los datos (criptografía), la estructura y secuencia lógica de los datos transmitidos, y los parámetros técnicos de identificación y autenticación de las partes de la comunicación, estas reglas procuran generalmente garantizar la confidencialidad, integridad, autenticación y el no repudio de la información transmitida.

Vigentes en los más diversos niveles funcionales de una red de telecomunicaciones, los protocolos permiten tanto la comunicación de los dispositivos físicos como de aplicaciones de software, gracias a que ponen en común las reglas que rigen el contenido de la comunicación, por lo que resulta natural que puedan contribuir en el futuro a los sistemas internacionales de protección de datos personales (Simpson & Foltz, 2016).

4.1.4. Protocolo de Plataforma de Preferencias de Privacidad (P3P)

Desarrollado por la *World Wide Web* Consortium (W3C) y recomendado desde el 26 de abril de 2002, el protocolo P3P establece un conjunto de reglas mediante las cuales los sitios web pueden declarar públicamente y mediante un formato estándar, sus intenciones de uso de la información que recopilan sobre sus usuarios (O'Brien & Weir, 2017).

El protocolo P3P propone un sistema mediante el cual tanto las páginas web como el usuario declaran los tipos de información que buscan recopilar,

mientras que los usuarios determinarán qué tipo de información están dispuestos a compartir (Simpson & Foltz, 2016).

A partir de estos datos el protocolo será capaz de informar al usuario en caso de que la página solicite más información de la que el usuario ha autorizado compartir y proporcionarle de esta manera la capacidad de tomar decisiones informadas con base en su derecho de autodeterminación informativa. En términos generales, P3P se preocupaba por facilitar al usuario la capacidad de conocer y decidir sobre los datos personales almacenados por el servidor, su uso, permanencia y visibilidad.

4.1.5. Protocolo *Do Not Track*

Propuesto originalmente en 2009, el protocolo *Do Not Track* basa su sistema de protección en la incorporación de un encabezamiento a las comunicaciones informáticas, el cual solicita que toda aplicación web que lo reciba desactive sus sistemas de rastreo de usuarios. Al igual que en el caso de P3P, a la fecha el protocolo *Do Not Track* no puede ser aun considerado como una solución viable a los problemas de la Protección de Datos Personales, en tanto no cuenta con un apoyo substancial por parte de la industria, a la vez que tampoco cuenta con un marco legal internacional que haga vinculantes sus solicitudes.

4.1.6. Privacy by Design (PbD)

Basado en siete principios fundamentales de la GDPR que son legalidad, equidad y transparencia, limitación del propósito, minimización de datos, exactitud, limitaciones de almacenamiento, integridad, confidencialidad y responsabilidad; el método de protección PbD procura brindar un enfoque holístico a la protección de los datos personales por medio de la implementación predeterminada de la privacidad a lo largo de todas las etapas de desarrollo e implementación de las nuevas tecnologías. Así, la privacidad por diseño “se extiende a una “Trilogía” de aplicaciones que engloban:

sistemas de tecnologías de la información, prácticas de negocio responsables y diseño físico e infraestructura en red (Cavoukian, 2011).

4.2. Responsabilidad de los entes en la protección de datos personales

La ley europea de protección de datos otorga derechos individuales en relación con los datos personales, como el derecho a la transparencia y derecho a solicitar acceso, corrección o borrado de la información.

Legalmente hablando, estos derechos se otorgan en relación con las organizaciones a cargo del procesamiento de datos, los llamados controladores de datos. Por lo tanto, para que el sistema de derechos funcione, debe ser posible determinar quién cuenta con el control de datos. Al final, es el controlador de datos el que tiene obligaciones para con el dueño de la información.

El Reglamento General de Protección de Datos (RGPD) exige que las empresas sean transparentes sobre los datos personales que tienen sobre sus clientes, es decir, deben informar para qué usan esos datos con el objetivo de ofrecer al usuario un mayor control sobre el procesamiento de su información.
Esto comienza con una política de privacidad sólida y fácil de seguir, y asegurando que haya determinado la base legal adecuada para procesar los datos de los clientes. De la misma forma, un controlador de datos se refiere a la persona o personas que determinan el propósito (por qué) y los medios (cómo) del procesamiento de datos personales. Por ejemplo, cualquier empresa que recopile información sobre personas vivas es, en esencia, un controlador de datos.

Por otro lado, un procesador de datos se refiere a la persona o personas que reciben instrucciones para procesar datos personales en nombre del controlador. El procesamiento cubre tanto el almacenamiento como el uso de datos personales.

4.3. El principio de responsabilidad proactiva

El artículo 5.2 del RGPD, incorpora la exigencia directa de este texto normativo a cualquier persona que realice un tratamiento de datos personales, salvo excepciones. Esto es el llamado principio de responsabilidad activa, por medio del cual se le obliga al responsable del tratamiento de los datos, no solo el cumplimiento de los principios relativos al tratamiento de estos, sino también se le exige que esté en la capacidad de demostrar que cumple con ellos y la normativa en materia de protección de datos de carácter personal.

Es decir, que el responsable o encargado del tratamiento debe ser proactivo y demostrar en todo momento su cumplimiento. Inclusive, autores como Cavoukian, señalan una relación directa de este principio con el de PbD, en aquellos casos en que no esté claro la necesidad o el uso de la información relativa a una persona, se debe adoptar siempre una posición que resguarde mayormente la privacidad de los datos.

4.4. Competencia del responsable del tratamiento de datos y PbD

EL RGPD establece las distintas responsabilidades que asume el tratante de los datos, entre las que se indican medidas organizativas y de carácter técnica con el fin de asegurar la protección de la información. Entre estas medidas se establece que el responsable debe aplicar las políticas relacionadas a la protección de datos.

“Resulta trascendental en el nuevo paradigma de la protección de datos que cobija el RGPD pues implica la transición del simple cumplimiento de la normativa de forma reactiva por parte de los responsables y encargados de tratamiento de los datos personales, a un sistema en que se exige que estas personas demuestren efectivamente la diligencia en la adopción de medidas tendientes al cumplimiento de las obligaciones dispuestas en la nueva regulación.” (Álvarez, 2017, pág. 15)

Lo que representa que la obligación del cumplimiento de lo establecido en la RGPD por parte de los entes responsables pasa de ser pasivo a forzar de forma legal su cumplimiento y la subsecuente demostración de los esfuerzos traducidos en acciones demostrables cuyo único fin sea la protección efectiva de datos personales.

4.5. Encargado de la protección de datos

En su artículo 37 el RGPD crea la figura del delegado de protección de datos, para los casos en que el tratamiento lo lleve a cabo una autoridad u organismos públicos, con excepción de los tribunales que actúen en ejercicio de su función judicial, cuando el tratamiento de datos en virtud de su naturaleza, alcance los fines requiera de una observación habitual y sistemática de datos de interesados a gran escala, o, las actividades consistan en el tratamiento de categorías especiales de datos y datos relativos a condenas e infracciones penales.

Como bien lo indica la Agencia Española de Protección de Datos (AEPD), este constituye uno de los elementos claves del Reglamento y es un garante a su vez de la normativa de protección de datos sin que ello llegue a suponer un relevo en las funciones encomendadas a las autoridades independientes de control (AEDP, 2014).

Es obligación del responsable y el encargado del tratamiento de datos procurar que el delegado participe de forma adecuada y oportuna en todos aquellos aspectos relacionados con la protección de datos personales. Además, deberán facilitar los recursos necesarios para el desempeño de las labores, así como acceso a los datos personales y las operaciones de tratamiento.

Adicionalmente, el artículo 39 garantiza al delegado no recibir instrucciones en el desempeño de sus funciones y únicamente rendir cuentas al más alto nivel jerárquico del responsable o encargado del tratamiento.

Dentro de las funciones del delegado se encuentran las mencionadas en el artículo 39, las cuales comprenden informar y asesorar al responsable, encargado y empleados que realicen el tratamiento, de sus obligaciones en virtud del RGPD y las disposiciones locales; en otras palabras, supervisar el cumplimiento de lo dispuesto en el RGPD; ofrecer asesoramiento sobre la evaluación de impacto relativa a la protección de datos; cooperar con la autoridad de control; y, actuar como punto de contacto de la autoridad de control competente.

4.6. Responsables de la tecnología Caso Facebook

La empresa Facebook emitió un comunicado el 29 de enero del 2018, estableciendo lo siguiente:
“Estamos comprometidos con la transparencia, el control y la responsabilidad, de la siguiente manera:

Transparencia: nuestra Política de datos seguirá siendo el lugar único y consolidado en el que se trazan las directrices para el uso de datos y el procesamiento de datos personales. Asimismo, ofreceremos capacitación mediante experiencias de consentimiento para los usuarios nuevos y existentes, notificaciones en los productos y una campaña para dar a conocer la normativa a los consumidores.

Control: seguiremos proporcionando herramientas para que las personas puedan controlar la manera en que se usan sus datos. Como complemento, estamos simplificando el diseño de la configuración de privacidad en un nuevo centro de control. Además, proporcionaremos opciones de repaso mientras las

personas usan Facebook, por ejemplo, recordatorios que aparecerán en la sección de noticias indicándoles cómo comprobar bien la configuración.

Responsabilidad: somos responsables de nuestras prácticas de privacidad, lo que incluye la actualización del programa de cumplimiento actual para garantizar que nuestra revisión y cumplimiento del GDPR se documenten adecuadamente. Además, nos reunimos con autoridades reguladoras, legisladores, especialistas y académicos de todo el mundo para conocer su opinión.” (facebook, 2018)

Ante lo anterior expuesto, la posición que ostentan las redes sociales parecen claras con respecto al tratamiento de datos de los usuarios, las obligaciones y responsabilidades en materia de protección de datos que éstos deberían asumir. Además, dan lugar a una mayor discusión, pues es fundamental que las redes sociales sean claras y transparentes en sus políticas de uso y privacidad, con el fin de informar correctamente a los usuarios de cuáles son sus derechos y deberes para llevar a cabo un uso responsable de las plataformas, sin poner en riesgo sus propios derechos ni los de terceros.

4.7. Responsabilidad de los usuarios en la protección de datos

La mayor responsabilidad sobre la administración de los datos personales recae sobre los usuarios, los cuales son los encargados de suministrar la información a través de ficheros, dentro de los elementos que intervienen en los sistemas de comunicaciones, los usuarios representan el mayor volumen y el grupo que menos tiene conciencia sobre el uso y disposición de los datos.

4.8. La responsabilidad en la propuesta de ley de protección de datos en Ecuador

El artículo 11 del proyecto de ley asigna la autoridad de protección de datos a la Dirección Nacional de Registro de Datos Públicos, órgano adscrito al Ministerio de Telecomunicaciones y Sociedad de la Información:

"Art. 11.- Autoridad Nacional de Protección de Datos Personales. La Dirección Nacional de Registro de Datos Públicos adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información será la Autoridad Nacional de Protección de Datos Personales y ejercerá la vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley". (Asamble Nacional de Ecuador, 2016)

La Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales entraría en conflicto directo con la Ley del Sistema Nacional del Registro de Datos Públicos. En caso de conflicto de leyes, al menos en teoría, prevalecería la ley orgánica, aunque podríamos predecir que será necesaria una reforma (Álvarez, 2017).

En conclusión según lo planteado en la ley tienen responsabilidad en la comunicación y tratamiento de los datos no solo las personas jurídicas sino también autónomos, *freelancers*, asociaciones, colectivos y personas propietarias de un blog, etc., a través del cual se recojan datos de terceros para realizar consultas y para cualquier otra transacción.

5. CAPÍTULO V. RECOMENDACIONES TÉCNICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR

La directora nacional de Registro de Datos Públicos (DINARDAP), Mgs. Lorena Naranjo Godoy (2017), explicó el rol que tiene el "Estado como responsable de

los datos personales", e indicó que todo este potencial (datos personales) que mueve las economías y que permite tomar mejores decisiones, no ha podido ser regulado en Ecuador.

Textualmente, dice que "nuestro país es el claro ejemplo de normativa con enfoque sectorial, es decir, existen varias normas dispersas que aparecen en leyes específicas". Además, según su criterio, los principales retos que "tenemos como Estado es no desactualizarnos más aún de lo que estamos, para no aislarnos a escala internacional, y generar la Ley de Protección de Datos" (DINARDAP, 2017).

Finalmente, se concluye estableciendo que Ecuador necesita una ley de protección de datos personales con visión técnica. Por otro lado, los puntos principales que formarán parte de la normativa presentada se deben enfocar en los siguientes aspectos: derechos, régimen especial de datos personales, seguridad y protección de datos y régimen sancionatorio. En resumen, los principales puntos del anteproyecto de ley deben legitimar lo siguiente:

a) Reconocimiento de diferentes principios para la aplicación de la ley en el tratamiento de datos personales, tales como legalidad, lealtad, legitimidad, finalidad, entre otros.
b) Reconocimiento de derechos a favor de los titulares de los datos, tales como el derecho a la transparencia, derecho al acceso, derecho de eliminación de datos, entre otros.
c) Establece un régimen especial para datos sensibles, datos de niños, adolescentes, etc.
d) Establece un régimen de seguridad y protección de datos personales.
e) Regula la transferencia internacional de datos.
f) Establece obligaciones para los responsables y encargados del tratamiento de datos.
g) Establece un régimen de infracciones tales como la falta de notificación a las vulneraciones de seguridad, utilización de información o datos para

fines distintos a los declarados, no implementación de políticas de protección de datos personales en las empresas, etc.

El objetivo de la ley debe ser crear un destino más seguro para el tratamiento de datos personales y un territorio donde sus ciudadanos nacionales o extranjeros tengan la convicción de que sus datos están seguros y protegidos.

5.1. Transferencias internacionales de datos e inversión extranjera

Las transferencias internacionales de datos son, en nuestra sociedad globalizada, un elemento clave para la prestación de servicios. En términos generales, las transferencias internacionales de datos pueden involucrar el flujo de datos personales de territorios o estados donde las regulaciones de protección de datos se aplican a áreas con normas más flexibles.

Además, estas transferencias corresponden a una actividad estratégica que es importante para el crecimiento y desarrollo de las empresas. Al crear una empresa dedicada a actividades comerciales o de servicios, es importante el hecho de que sus operaciones se realicen en un país donde se garantice la privacidad de los datos.

El principio general de transferencia internacional de datos determina que este tipo de traspasos se realizarán si los países cumplen con las disposiciones establecidas en sus regulaciones nacionales. En este sentido, se concluye si un país u organización internacional garantiza un nivel adecuado de protección de datos / información. Además, el nivel de protección de los derechos y libertades de las personas físicas no debe verse afectado.

Por tanto, el camino correcto a tener en cuenta es que Ecuador debe considerarse como un destino propicio para la inversión. Un primer paso ya se ha dado, debido a que el gobierno ya ha iniciado el proceso de implementación de la legislación de protección de datos. Así, una vez que la ley sea efectiva, las compañías extranjeras pueden confiar en que Ecuador es una jurisdicción

dedicada a la protección de datos.

5.2. Aspectos técnicos del RGPD y su cumplimiento en el Proyecto de Ley de Protección de Datos en Ecuador

La principal forma de cumplir con todos los requisitos del RGPD es procesar el anonimato de los datos. El RGPD considera que un conjunto de datos es anónimo cuando la reidentificación solo es posible con un gran esfuerzo o medios poco probables.

Los datos totalmente anónimos son información que no pueden identificar de ninguna manera a una persona, ya sea directamente a través del nombre y el número de identidad nacional, o indirectamente a través de variables de fondo, lista de nombres, clave de aleatorización, fórmula o código de cifrado. Para el procesamiento de datos personales, el RGPD define una serie de requisitos legales, organizativos y técnicos, y propone diferentes métodos.

En primer lugar, en la mayoría de los casos, el procesamiento de datos personales solo se permite si el interesado ha dado su consentimiento (Artículo 6) Se aplican excepciones cuando el procesamiento de datos está explícitamente permitido por una ley o regulación, o garantiza "intereses vitales del sujeto de datos" (Comisión Europea, 2014).

El artículo 5 establece que el consentimiento otorgado debe limitarse a un propósito específico para el procesamiento de datos. También, el controlador de datos (la entidad responsable de recopilar los datos) no puede fingir un propósito de procesamiento de datos demasiado genérico ni cambiar el propósito de forma arbitraria, de la misma forma indica el mismo artículo, que otro principio de procesamiento de datos es la minimización que se refiere a limitar la recopilación, el almacenamiento y el uso de datos personales a datos relevantes, adecuados y lo que es más importante, necesarios para llevar a cabo el propósito para el cual se procesan los datos.

Cabe destacar que la seudonimización se menciona explícitamente como una medida de minimización de datos. En los datos seudonimizados, los parámetros identificables se reemplazan por otros identificadores generados, de forma aleatoria. Esto generalmente no tiene ningún impacto negativo en el proceso de extracción de datos y, preferiblemente, debe ser iniciado por el controlador de datos antes de transferir la información al procesador de datos.

Los resultados del procesamiento de datos deben estar vinculados mediante el controlador de datos, pues éste contiene los seudónimos de mapeo (también conocidos como tablas de pseudo búsqueda).

Además de los datos anónimos, el almacenamiento en el controlador de datos debe cumplir con el GDPR mediante el empleo de técnicas que protegen los datos en reposo (por ejemplo, cifrado y control de acceso estricto). Además, el GDPR en su artículo 32 establece que requiere "medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo" (Comisión Europea, 2014), que comúnmente incluye la aplicación de técnicas como el cifrado de datos, el control de acceso, la protección física y nuevamente la seudonimización. Una extensión del principio de minimización de datos es el principio de limitación de almacenamiento, que restringe la duración de la reserva de información a un período específico.

En el contexto del procesamiento de datos, el artículo 22 de la GDPR indica que debe tenerse más en cuenta que los procesos de toma de decisiones automáticos tienen un impacto en los individuos, un ejemplo de ello son los datos biométricos que requieren el consentimiento explícito del interesado.
Se recomienda que para cumplir en términos técnicos, la propuesta de Ley de Protección de Datos en Ecuador debe establecer los mecanismos técnicos para preservar la privacidad de los usuarios mediante el anonimato de los datos personales.

El primer paso para anonimizar la información de forma correcta es analizar

cómo es la disposición de la base de datos a la que se quiere dar acceso, y clasificar toda la información en las siguientes categorías:

- **Datos sensibles**: son los datos que presentan un cierto valor. Se trata de información sobre la cual se extraerán conclusiones en un análisis posterior (condición médica, salarios, etc.).
- **Identificadores:** son aquellos campos de la base de datos que permiten identificar a una persona de forma única, como puede ser la cédula de identidad, teléfono celular, etc.
- **Cuasi-identificadores:** son todos los demás datos, es decir, aquellos datos personales que no son identificadores, y que en principio no tienen un valor especial para su análisis. Además, por sí solos no revelan información, pero cuando se combinan entre ellos o con otras fuentes externas de datos pueden llegar a desvelar nuestra identidad.

Por otro lado, se establecen los siguientes métodos como los más comunes para el anonimato de datos:

- **Supresión:** eliminar completamente los valores de un atributo o reemplazarlos con un valor ficticio (generalmente un asterisco "*"). Esta operación generalmente se realiza en identificadores explícitos.
- **Generalización:** reemplazo de valores con términos más generales o más abstractos dentro de la taxonomía de atributos, por ejemplo, fecha de nacimiento → edad (en años); código postal → primeros dos dígitos del código ZIP. Esta operación generalmente se emplea con el uso de cuasi-identificadores.
- **Permutación:** partición de los datos en grupos y mezcla los valores sensibles dentro de cada grupo. Como consecuencia, se elimina la relación entre los cuasi-identificadores y los datos sensibles.
- **Perturbación:** se reemplazan los valores de manera que se elimina el vínculo con los datos originales, pero se mantienen las propiedades estadísticas similares. Narayanan & Shmatikov (2008).

De la misma forma, hay que aclarar que la propuesta de protección de datos en Ecuador no debe establecer un método específico para el anonimato de datos, pero debe incluir todos los aspectos antes mencionado a fin de cumplir con lo establecido en el RGPD y así asegurar que los entes regulatorios dispongan de una visión técnica relacionada a la protección de datos personales.

Es de gran importancia establecer dentro del proyecto de ley que se debe realizar una evaluación del impacto de la protección de datos y administración de datos confidenciales en las primeras etapas de cualquier proyecto relacionado con el desarrollo o implantación de nuevas tecnologías en el país; con el fin de identificar posibles desafíos de privacidad y procurando siempre la conservación de la información, para lo cual se debe incluir en el proyecto un responsable únicamente de evaluar estos aspectos, además de aplicar la seudonimización o cifrado de los datos.

En función del artículo 29 desarrollado por la Comisión Europea (CE) en el año 2014, un grupo de trabajo sobre protección de datos estableció el dictamen 05/2014 sobre técnicas de anonimización, instituyendo que se reconoce el valor potencial de la anonimización, en particular como estrategia para permitir a las personas y la sociedad en su conjunto beneficiarse de los datos abiertos al mismo tiempo que se mitigan los riesgos para los interesados, los responsables del tratamiento deben considerar distintos aspectos y valorar todos los medios que puedan utilizarse razonablemente para la identificación de los datos (ya sea por el responsable del tratamiento o por terceros).

La conclusión del presente dictamen es que las técnicas de anonimización pueden aportar garantías de privacidad y usarse para generar procesos de anonimización eficientes, pero solo si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener la anonimización deseada al mismo tiempo que se generan datos útiles.

5.3. Metodología propuesta para aplicar la anonimización de los datos

El objetivo de la presente metodología es direccionar el accionar de los entes responsables del tratamiento en la forma como debe realizarse la protección de datos desde un punto de vista técnico, se establecen los pasos que deben realizar para lograr el cumplimiento de la norma:

a) Determinar el modelo de lanzamiento. Esto se refiere a cómo se lanzará el conjunto de datos anonimizados pudiendo ser estos públicos o no públicos. Público se refiere a ponerlo a disposición de prácticamente cualquier persona, no público a una liberación controlada o limitada de destinatarios conocidos. El modelo de lanzamiento público plantea inherentemente más desafíos en las técnicas de anonimización, debido a que se tendrá menos control sobre quien accede a estos datos y en consecuencia se incrementa su uso sin consentimiento.
b) Determinar el umbral de riesgo de re-identificación aceptable, así como la utilidad esperada y el umbral de riesgo previsto o requerido. Considerando que el umbral de riesgo establecido en esta etapa debe distinguirse claramente si los controles adicionales se toman en consideración o solo reflejan el riesgo de los datos.
c) Clasificar los atributos de los datos. Se trata de clasificar los atributos en el conjunto de datos como identificadores directos, identificadores indirectos o no identificadores, lo que afecta a cómo se procesarán los atributos posteriormente.
d) Eliminar los atributos de datos no utilizados: En el proceso de anonimización, por lo general, la mayoría de los atributos, ya sean identificadores directos o indirectos, requieren procesamiento o al menos consideración, para que se vuelvan menos identificativos. Por lo tanto, cualquier atributo que claramente no sea requerido en el conjunto de datos anonimizados debe ser suprimido, para evitar su uso posterior y posible reidentificación.

e) Anonimizar identificadores directos e indirectos. Esto se hace mediante la aplicación de técnicas antes descritas. Diferentes técnicas son aplicables para los tipos de identificadores. Algunas técnicas pueden (y con frecuencia, deben) usarse en combinación.
f) Realizar más anonimización, si es necesario. Si el riesgo real es mayor que el umbral, se requiere una anonimización más fuerte.
g) Evaluar la solución. Esto incluye examinar el conjunto de datos anonimizados para evaluar si la utilidad cumple con el objetivo. Si la utilidad es insuficiente, el proceso de anonimización debe ser rediseñado o puede considerarse si la anonimización es factible para este conjunto de datos.
h) Determinar los controles requeridos para asegurar que se está protegiendo los datos, en la actualidad existen múltiples elementos para realizar control, estos pueden ser técnicos como la anonimizacion o el cifrado y no técnicos como medidas legales y organizativas, los entes deben determinar en función del tipo de organización y el tipo de datos que manejan cuales son los controles adecuados para su institución y para lograr la protección de los datos.
i) Documentar el proceso de anonimización. Los detalles del proceso de anonimización, los parámetros utilizados y los controles deben ser registrados claramente para futuras referencias. Dicha documentación facilita la revisión, el mantenimiento, el ajuste fino y las auditorías. Tomando en consideración que dicha documentación debe mantenerse de forma segura, ya que la publicación de los parámetros puede facilitar la re-identificación.

En la figura 2, se muestra la propuesta para una metodología sobre el proceso de anonimización que deben realizar los responsables para la protección de datos personales, se divide en dos etapas, con la finalidad de poder evaluar el nivel de cumplimiento en función de los elementos logrados dentro del procedimiento y así otorgar un estatus a las empresas (etapa de pre-anonimización o anonimización).

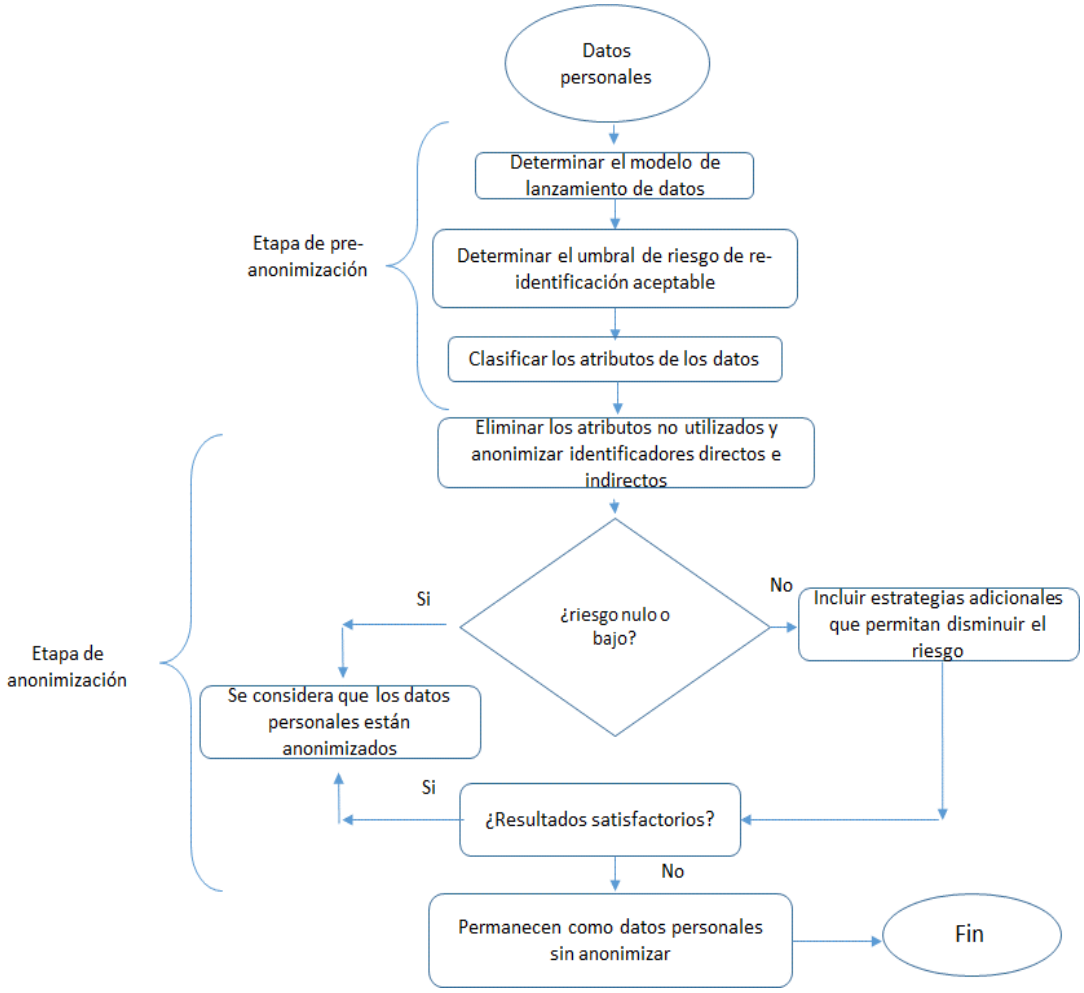

Figura 2. Metodología propuesta para el procedimiento relacionado a la anonimización de datos

Los elementos técnicos que deben incorporarse al proyecto de ley de protección de datos en Ecuador se pueden resumir en los siguientes aspectos:

- Los responsables del tratamiento deben revelar la técnica o el conjunto de técnicas de anonimización que se hayan utilizado, sobre todo si tienen la intención de publicar el conjunto de datos anonimizado.
- Deben eliminarse del conjunto de datos los atributos obvios (es decir, los raros) y los cuasi identificadores.
- Otro punto a tener en cuenta es que el riesgo de la re-identificación con el tiempo puede aumentar o cambiar, como también puede suceder con

la tecnología, por lo que se recomienda que si se procede a la regulación, esta debe considerar la presencia en su articulado del principio de neutralidad tecnológica, es decir que debe ser neutro en cuanto a la tecnología que se regula y pensar en la posible evolución que esta pueda experimentar.

5.4. Propuesta de modificación del Proyecto de Ley para la Protección de Datos en Ecuador

En función a lo anteriormente expuesto, a continuación se redactan y presentan los artículos que deben incorporarse en el proyecto de ley que actualmente desarrolla el Ecuador, a fin de concentrar los aspectos técnicos relacionados a cómo debe realizarse la protección de datos por los entes responsables en base a la metodología desarrollada en la Figura 2:

a) Artículo 4. Definiciones

Se recomienda incluir las siguientes definiciones técnicas:

Anonimización de datos personales

La "anonimización" de los datos significa procesarlos con el objetivo de evitar de manera irreversible la identificación de la persona con quien se relaciona. Los datos se pueden considerar de manera efectiva y lo suficientemente anonimizados si no se relacionan con una persona física identificada o identificable o cuando se ha convertido en anónimo de tal manera que el sujeto de los datos no es o ya no es identificable.

Seudonimización de datos personales

Es aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

b) TITULO II. Derechos y obligaciones en la protección de datos

Se recomienda incluir el siguiente artículo:

Artículo 8. Obligaciones del responsable del tratamiento de la información. Incluir el Inciso 6. Aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que en su caso incluya.

c) TITULO VII. Anonimación de datos personales

Se recomienda incluir los siguientes artículos:

Articulo 29.- Definición

La anominación de datos corresponde a aquellas medidas técnicas y organizativas apropiadas aplicadas de manera efectiva para integrar las salvaguardas necesarias en el procesamiento para cumplir con los requisitos de este Reglamento y proteger los derechos de los interesados.

Articulo 30.- Responsable de la anonimación

El responsable del tratamiento de la información que comience el proceso de apertura de datos debe documentar, las diferentes etapas del proceso de anonimización para obtener un control y resultado óptimos y evitar el posible riesgo de reidentificación.

Articulo 31.- Etapas del proceso de anonimación

El proceso de anonimación constará de tres etapas; preanonimización, anonimización y control.

Preanonimización: En la etapa se diseña el proyecto de anonimización, en el que se deberán identificar con claridad las variables, los identificadores directos e indirectos, los datos confidenciales, cuál o cuáles serán las técnicas adecuadas de anonimización, según el conjunto de datos de que se trate, el riesgo de reidentificación asociado, finalizando con la ejecución del proyecto.

Anonimización: El objetivo final es proveer los datos desagregados para que el público en general pueda utilizarlos, sin generar conflictos con los titulares de los datos, para la anonimización se deberá aplicar técnicas, algoritmos, pruebas de calidad y entregar el resultado al responsable para su aprobación.

Control: se deberá realiza controles periódicos por parte de los técnicos en virtud de la aparición de las nuevas tecnologías y métodos para prevenir y evitar los posibles riesgos de reidentificación.

Articulo 32.- Técnicas de anonimación

En el presente proyecto se establecerán las posibles técnicas para efectuar la anonimación, sin ser de estricto cumplimiento, pero debe asegurarse y registrarse el método utilizado para la protección de los datos

Los conjuntos de técnicas de anonimización se dividen en generales y particulares y dentro de los generales se encuentra la aleatorización y la generalización. La aleatorización se subdivide en adición de ruido, permutación, y privacidad diferencial; la generalización en agregación, anonimato k, diversidad l y proximidad t.

Definición de términos:

- **Aleatorización:** es una familia de técnicas que altera la veracidad de los datos para eliminar el fuerte vínculo entre los datos y el individuo. Si los

datos son suficientemente inciertos entonces ya no pueden ser referidos a un individuo específico. (Comisión Europea, 2014)

- **Adición de ruido:** La técnica de adición de ruido es especialmente útil cuando los atributos pueden tener un efecto adverso importante en los individuos y consiste en modificar los atributos en el conjunto de datos de tal manera que sean menos precisos y al mismo tiempo conserven la distribución general. Al procesar un conjunto de datos, el observador asumirá que los valores son precisos, pero esto solo será cierto hasta cierto punto. (Comisión Europea, 2014)
- **Permutación:** consiste en barajar los valores de los atributos en una tabla para que algunos de ellos estén vinculados artificialmente a diferentes sujetos de datos, es útil cuando es importante mantener la distribución exacta de cada atributo dentro de la base de datos. (Comisión Europea, 2014)
- **Privacidad diferencial:** se enmarca dentro de la familia de técnicas de aleatorización, con una diferente enfoque: mientras que, de hecho, la inserción de ruido entra en juego de antemano cuando se supone que se publica el conjunto de datos, se puede usar la privacidad diferencial cuando el controlador de datos genera datos anónimos mientras se conserva una copia de los datos originales. Dichas vistas anónimas se generarían normalmente a través de un subconjunto de consultas para un tercero en particular. (Comisión Europea, 2014)
- **Generalización en agregación:** es la segunda familia de técnicas de anonimización. Este enfoque consiste en generalizar, o diluir, los atributos de los sujetos de datos mediante la modificación de la escala respectiva o el orden de magnitud (es decir, una región en lugar de una ciudad, un mes en lugar de una semana). Mientras que la generalización puede ser efectiva para prevenir el aislamiento, no permite anonimización en todos los casos; en particular, requiere enfoques cuantitativos específicos y sofisticados para prevenir la vinculación y la inferencia. (Comisión Europea, 2014)

- **Anonimato K:** tienen como objetivo evitar que un sujeto de datos sea individualizado, agrupándolos con, al menos, k otras personas. Para lograr esto, los valores de los atributos se generalizan en una medida tal que cada individuo comparte el mismo valor. (Comisión Europea, 2014)
- **Diversidad L:** extiende el anonimato k para asegurar que los ataques de inferencia deterministas ya no sean posible asegurándose de que en cada clase de equivalencia cada atributo tenga al menos l diferentes valores. Un objetivo básico a lograr es limitar la ocurrencia de clases de equivalencia con un atributo de pobre variabilidad, de modo que un atacante con conocimiento de fondo sobre un sujeto de datos específico siempre presente con una incertidumbre significativa. (Comisión Europea, 2014)
- **Proximidad T**: es un refinamiento de la diversidad de l, ya que apunta a crear clases equivalentes que se asemejan a la distribución inicial de atributos en la tabla. Esta técnica es útil cuando es importante mantener los datos lo más cerca posible del original; para ello, se coloca una restricción en la clase de equivalencia, es decir, que no solo al menos l valores diferentes debe existir dentro de cada clase de equivalencia, pero también que cada valor se representa tantos veces como sea necesario para reflejar la distribución inicial de cada atributo. (Comisión Europea, 2014)

Finalmente, deben adoptarse buenas prácticas para minimizar los riegos que puedan aparecer con la anonimización y quienes realicen el tratamiento de los datos, (responsables), deben concentrar su atención en los medios que serían necesarios para la reidentificación, principalmente en lo que atañe a los conocimientos asociados al uso de dichos medios, a la valoración de la probabilidad y gravedad del uso, a la tecnología disponible al le puede ocasionar.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

De la investigación realizada sobre los sistemas de protección apara los datos personales que en la actualidad se aplica en las tecnologías de telecomunicaciones, se determinó que las mismas presentan importantes deficiencias técnicas, por lo que el riesgo relacionado al uso de los datos sin la autorización del propietario está vigente en el Ecuador.

El marco regulatorio relacionado a la protección de datos se encuentra en constante crecimiento, considerando que el GDPR entró en vigor después de un período de implementación de dos años; la tendencia mundial se dirige al desarrollo de importantes de leyes en términos de privacidad, no obstante Ecuador se encuentra en la actualidad en discusión sobre una propuesta de ley desarrollada y presentada por el estado.

Al realizar una evaluación de la propuesta de ley en Ecuador, se ha detectado una serie de vacíos regulatorios, principalmente en lo que refiere a las responsabilidades de los entes relacionados al tratamiento de datos, sin establecer una metodología concerniente al proceso de anonimización de datos.

El principal riesgo relacionado uso de información personal sin la autorización del propietario corresponde a la revelación de información que pueda afectar la integridad moral, seguido del riesgo de sufrir estafas y daños informáticos tales como el *pishing.*

Para el control de los datos existen varias técnicas a través de las cuales se generan diferentes grados de ruptura del vínculo entre el dato y la identificación de su titular produciendo la anonimización de los datos, cada ente debe evaluar la técnica que se adapte a sus condiciones particulares y que logre con éxito la protección del dato.

La anominización se considera un mecanismo que permite la protección de los datos, su aplicación en los sistemas de información debe ser registrada y controlada a través de la propuesta de ley de protección de datos personales en Ecuador, con la finalidad de confirmar su implantación en los sistemas de transmisión de información.

Los responsables o encargados del tratamiento de los datos deben considerar que aun cuando se aplican medidas para la anonimización de datos, existen riesgos residuales por lo que se deben tomar medidas para prevenir la reidentificación al titular del dato.

Las técnicas de anonimización pueden aportar garantías a la protección de datos personales siempre que su aplicación se diseñe en forma adecuada, por lo que se deben tener en cuenta las etapas del proceso de anonimización (preanonimización, anonimización y control).

La propuesta de protección de datos en Ecuador no establece un método específico para el anonimato de datos, ni determina las medidas técnicas y organizativas apropiadas que deben aplicar los entes responsables de los datos para garantizar un nivel de seguridad adecuado al riesgo que determine el caso.

Dentro del proyecto de ley se debe establecer la necesidad de realizar una evaluación del impacto de la protección de datos y administración de datos confidenciales en las primeras etapas de cualquier proyecto relacionado con el desarrollo o implantación de nuevas tecnologías en el país.

Un impulso importante para las inversiones extranjeras corresponde a generar una jurisdicción adecuada, por lo que es determinante las subsecuentes discusiones que permitan concluir con un reglamento de protección de ley aprobado y promulgado que ubique a Ecuador como país garante de la protección de datos personales.

6.2. Recomendaciones

Ecuador como país debe realizar gestiones gubernamentales de alto nivel con el fin de solicitar que las tecnologías disponibles y en uso en la actualidad, realice acciones inmediatas con el fin de mejorar sus sistemas internos a fin de garantizar la protección de datos personales a los ciudadanos.

Se debe realizar una revisión a profundidad de los términos establecidos en la propuesta de Ley de Protección de Datos, previo a su aprobación para lo cual sebe involucrar a los elementos técnicos, como proveedores del servicio y especialistas en el área de telecomunicaciones.

Este proyecto debe completarse con un programa apoyado por el estado Ecuatoriano para la formación a las personas sobre el manejo de sus datos, así como la importancia de tomar precauciones para la entrega de información personal en cualquier ámbito tecnológico.

Se recomienda que los responsables de tratamiento de los datos, incorporen buenas prácticas para minimizar los riegos que puedan aparecer con la anonimización.

REFERENCIAS

Álvarez, L. E. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Revista de Derecho FORO*, 43-61.

AEDP. (2014). Proteccion de dato y prevencion de delitos. España: AEDP.

Alarcon, J. (2018). Protección de datos personales en el mundo. Recuperado de http://www.deimosestadistica.com/dia-mundial-la-proteccion-datos/

Aristizábal, C., & Arias, J. (2011). El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. *Semestre Económico, volumen 14, N° 28, ISSN 0120-6346,*, 95-110.

Asamblea Nacional de Ecuador. (2016). Propuesta de Ley Orgánica de Protección de los derechos a la Intimidad y Privacidad sobre los Datos Personales. Recuperado el 10 de febrero de 2019 de http://www.fundamedios.org/wp-content/uploads/2016/09/proyecto-ley-de-datos.pdf

Asamblea Nacional de Ecuador. (2015). Ley Orgánica de Telecomunicaciones (LOT). Recuperado el 16 de febrero de 2019 de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

Baladán, F., Betarte, G., Blanco, A., Montaña, C., & Muracciole, B. (2016). Privacy by Design: de la abstracción jurídica a la práctica ingenieril. *Governance and Technology Series*, 139-161.

Barinas, D. (2013). El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. *RECPC 1.* http://criminet.ugr.es/recpc. ISSN 1695, 27-28.

Barriuso, C. (2009). Las redes sociales y la protección de datos hoy. Anuario Facultad de Derecho – Universidad de Alcalá II. https://core.ac.uk/download/pdf/58906859.pdf, 301-338.

Batalla, A. R. (2011). Tecnología, libertad y privacidad. Valencia, España: Publicaciones de la Universidad de Valencia.

Berners, T. (2016). Semantic Web and Web 3.0. *Conference presentation, International Semantic Web Conference*, 63-69.

Berrocal, A. (2016). La firma electrónica y su regulación en la ley 59/2003, de 19 de diciembre, de firma electrónica. *Foro, Nueva época, núm. 3*, 397-465.

Briones, I. M. (2017). La protección de los derechos constitucionales de los datos personales y datos íntimos en el Código Orgánico General de Procesos. Guayaquil: UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL.

Caicedo, E. A. (2014). A Acción De *Hábeas Data* Como Una Garantía Jurisdiccional En La Constitución De 2008, Apliación Y Formas De Hacerla Efectiva En La Práctica . Quito, Ecuador: Pontificia Universidad Católica Del Ecuador.

Capo, L. (2015). Sistemas de Detección de Intrusos en Seguridad Informática. Tino-42. https://www.researchgate.net/publication/296486726, 1-10.

Cavoukian, A. (2011). *Privacy by Design: los 7 principios fundamentales.* Ontario, Canada: Bosch.

Chávez, A. D., & Espinoza, I. O. (2017). Implementación de un sistema de seguridad DLP *(data loss prevention).* Mexico: Universidad Nacional Autónoma De México.

Chen, S. (2010). PRIVACIDAD Y PROTECCIÓN DE DATOS: UN ANÁLISIS DE LEGISLACIÓN COMPARADA. Diálogos Revista Electrónica de Historia, vol. 11, núm. 1,, 111-152.

Comision Europea. (2007). *Press release: Privacy Enhancing Technologies (PETs).* Ginebra.

Comisión Europea. (2014). 0829/14/EN. Dictamen 05/2014 sobre Técnicas de Anonimización. Europa: Comisión Europea.

Congreso Nacional. (2002). Ley de comercio electrónica, firmas y mensajes de datos (Ley No. 67. RO/ Sup 557). Quito, Ecuador: Congreso Nacional.

Congreso Nacional. (2002). *No. 2002-67*. Ley de comercio electrnonico, firmas electronicas y mensajes de datos. Quito, Ecuador: Congreso Nacional.

Congreso Nacional del Ecuador. (2002). Disposiciones generales de la Ley No. 2002-67. Quito, Ecuador: Congreso Nacional del Ecuador.

Consejo de Europa. (1981). CONVENIO 108 del Consejo de Europa de 28-1-1981. Estrasburgo.

CORPECE. (2016). infodesarrollo. Quito, Ecuador: Corporacion Ecuatoriana de Comercio Electronico. Obtenido de http://www.infodesarrollo.ec/component/content

DINARDAP. (s.f.). Dirección Nacional de Registro de Datos Públicos. Recuperado el 10 de enero de 2019 de http://www.datospublicos.gob.ec/ecuador-necesita-una-ley-de-proteccion-de-datos-personales-con-vision-tecnica/

Domingo, J. (2014). El tratamiento de los datos personales en internet. eprints.rclis.org, 1-10.

Ecuador. (2008). Ley del Sistema Nacional de Registro de Datos Públicos. Quito, Ecuador: Ecuador.

Ecuador. (2008). Constitución de la República. Quito: Registro Oficial, No. 449.

Ecuador. (2014). Código Orgánico Integral Penal. Quito, Ecuador: Ecuador.

Ernst & Young's. (2011). *Data loss prevention.* USA: EYGM Limited. .

Europea, C. (2014). 0829/14/ES Dictamen 05/2014 sobre técnicas de anonimización. Bruselas, Bélgica: CE.

Facebook. (2018). facebook.com. Recuperado el 24 de marzo de 2019, de https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr

Gellert, R. (2015). Understanding Data Protection As Risk Regulation. *Journal of Internet Law, vol., 18, n. 11*, 1-6.

Guilayn, A. A., & Ruiz, J. M. (2016). Aspectos legales de las redes sociales. Barcelona, España: Bosch.

Hoven, J. v., & Blaauw, M. (2014). Privacy and Information Technology. USA: Stanford University.

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2009). Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. España: Agencia Española de Protección de Datos (AEPD).

Latorre, G. (2014). Análisis estático y dinámico de una muestra de malware en sistemas Microsoft Windows Xp para determinar qué efectos produce sobre un sistema infectado. Quito, Ecuador: Escuela Politecnica Nacional.

Lombarte, A. R. (2009). Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal. Madrid, España: Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

Lotero, N. H. (2016). Clasificación de los Datos Personales e Implicaciones Legales. Colombia: Universidad Pontifica Bolivariana.

Muñoz, L., Pardillo, J., Mazón, J., & Trujillo, J. (2016). Definición y validación de medidas para procesos ETL. Panama: Universidad Tecnológica de Panama.

Muquinche, R. A. (2016). Protección De Datos Personales En La Legislación ecuatoriana . Quito, Ecuador: Universidad Central de Ecuador.

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of LargeSparse Datasets. *IEEE Symposium on Security and Privacy*, 111–125.

O'Brien, M., & Weir, G. (2017). *Understanding digital certificates.* Reino Unido: Department of Computer and Information Sciences, .

Olguín, M., Rivera, I., & Pérez, P. (2016). Sistemas de Detección de Intrusos (Ids), Seguridad en Internet. Polibits, núm. 34, 31-36.

Pérez, G. S., & González, I. R. (2018). Leyes de Protección de Datos Personales en el Mundo y la Protección de Datos Biométricos – Parte I. Revista Seguridad, 478 - 479.

Peterson, J., Tschofenig, H., & Aboba, B. (2017). *The Role of the Internet Engineering Task Force (IETF) in Improving Privacy on the Internet. Massachusetts Institute of Technology*, 1-6.

Poch, M. P. (2004). Derecho y nuevas Tecnologias. España: Editorial UOC.

Presidente Constitucional de la República. (2016). Reglamento General a la Ley Organica de Telecomunicaciones. Quito, Ecuador: Decreto Ejecutivo 864.

Presidente Constitucional de la Republica. (2016). Reglamento General a la Ley Orgánica de Telecomunicaciones. Quito, Ecuador: Decreto Ejecutivo 864.

Pulido, E. Z. (2013). La Protección de Datos Personales en España : Evolución Normativa y Criterios de Aplicación. Madrid, España: Universidad Complutense De Madrid.

Ramírez, J., García, T., & Bocarando, J. (2016). Estudio descriptivo del malware en una dependencia académica de una institución pública de educación superior. UNAM, 36-42.

Recuero, P. (2017). Big Data con Privacidad. Telefónica Digital España, S.L.U .

Reinoso, A. P. (2014). Protección Legal De Datos Personales y a la Reserva De Información Personal, y Su Transferencia Sin Consentimiento De Su Titular. Quito, Ecuador: Pontificia Universidad Católica Del Ecuador.

Rendon, M. (2014). Prevención y minimización de fuga de información implementando DLP (*Data Loss*). Cuenca, Ecuador: Universidad del Azuay.

Republica de Ecuador. (2015). Código Orgánico General De Procesos, COGEP. Quito, Ecuador: Asamble Nacional de Ecuador.

Safianu, O., Twum, F., & Hayfron, J. (2016). *Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection*. *International Journal of Computer Applications (0975 – 8887) Volume 143 – No.5*, 8-13.

Salazar, J. (2011). Estado actual de la Web 3.0 o Web Semántica. Tecnologías de Información y Comunicación -UNAM. Revista Digital Universitaria. Volumen 12, Numero 11, 25-29.

Santos, D. G. (2005). Nociones Generales de la Ley Orgánica de Protección de Datos. Madrid, España: Tecnos.

Serrudo, C. S. (2016). Revelación de Identidades en Sistemas Anónimos. *bit @ bit Vol. 1. Nº 1.*, 27 – 32.

Simpson, W., & Foltz, K. (2016). *Enterprise Considerations for Ports and Protocols. Institute for Defense Analyses, 358.*

Taal, A., Le, J., Leon, A. P., Sherer, J., & Jenson, K. (2017). *Technological and Information Governance Approaches*. *Computer Science and Information Technology 5(1)*, 1-7.

Tahboub, R., & Saleh, Y. (2014). Sistemas de prevención de pérdida y pérdida de datos (DLP). *NNGT Journal: International Journal of Information Systems. Volume 1 J*, 13-19.

Taluja, S., Kumar, P., & Lal, R. (2012). *Network Security Using IP firewalls. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 8. ISSN: 2277 128X*, 348-351.

Terol, J. M. (2013). *Privacy by design, construcción de redes sociales garantes de la privacidad.* Valencia, España: Civitas.

Torres, M. (2017). DLP: prevención de fuga de información (*data loss prevention*). Colombia: Universidad Piloto de Colombia.

Volpato, S. (2016). El Derecho a la Intimidad y las Nuevas Tecnologías. Sevilla, España: Universidad de Sevilla.

Wang, Y., & Kobsa, A. (2008). *Privacy-Enhancing Technologies*. *Handbook LiabSec kobsa*, 1-30.

Wehner, C. (2015). *Deep packet inspection--Use cases, requirements and architectures—Part I. Emerson Network Power, Embedded Computing Division*, 1-2.