UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

Revisión de literatura del impacto tecnológico sobre la protección de datos de carácter personal orientada a la infraestructura

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: JORDY GUSTAVO MIRANDA GODOY

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Jordy Gustavo Miranda Godoy con documento de identificación N° 0930282744 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 9 de febrero del año 2024

Atentamente,

Jordy Gustavo Miranda Godoy
0930282744

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE

TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Jordy Gustavo Miranda Godoy con documento de identificación No. 0930282744, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Impacto tecnológico sobre la protección de datos de carácter personal orientada a la infraestructura en una empresa Courier situada en el Ecuador", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 9 de febrero del año 2024

Atentamente,

_____

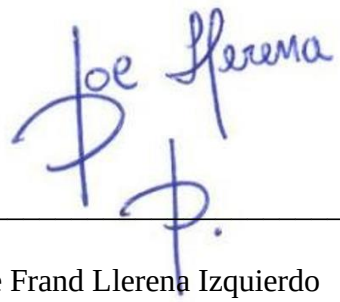
Jordy Gustavo Miranda Godoy
0930282744

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: IMPACTO TECNOLÓGICO SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL ORIENTADA A LA INFRAESTRUCTURA EN UNA EMPRESA COURIER SITUADA EN EL ECUADOR, realizado por Jordy Gustavo Miranda Godoy con documento de identificación N° 0930282744, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 9 de febrero del año 2024

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo a Dios y a cada uno de mis seres queridos, quienes han sido mis pilares para seguir adelante.

Es para mí una gran satisfacción poder dedicarles a ellos que con mucho esfuerzo, esmero y trabajo me lo he ganado

A mis Padres Iris Godoy & Javier Miranda, porque ellos son la motivación de mi vida mi orgullo de ser lo que seré.

A mi Tio Jairo Aguilar, sin duda algún recibí su apoyo incondicionalmente dándome motivación en cada una de mis ideas y poder brindarme esa seguridad en lo que podía llegar a lograr.

A mis hermanos Lissette & Abel, son la razón de sentirme orgulloso de culminar mi meta, gracias a ellos por confiar siempre en mi

En especial a Fabiana Zhindon siendo la mayor motivación en mi vida encaminada al éxito, fue el ingrediente perfecto para lograr alcanzar esta dichosa y muy merecida victoria en la vida, el poder haber culminado este articulo con éxito, y poder disfrutar del privilegio de ser agradecido, ser grato con esa persona que se preocupó por mí en cada momento y que siempre quiso lo mejor para mi porvenir te llevo siempre en mi corazón.

AGRADECIMIENTO

Agradezco a Dios por haberme permitido culminar mi carrera con éxitos con mucha salud y mucha sabiduría emprendiendo muchos conocimientos y poder lograr hacia mi futuro.

Gracias infinitas a mis padres, por su amor incondicional y su apoyo moral. Su fe en mí, incluso en los momentos más difíciles, ha sido el pilar de este logro. También expreso mi gratitud a mis hermanos, quienes supieron brindarme su tiempo para escucharme y apoyarme, a mis tíos, primos y amigos cercanos quienes supieron estar cuando más los necesitaba. Sin ustedes, todo esto no habría sido posible. Su amor y sacrificio han sido la luz que guio mi camino a través de este viaje académico.

Le agradezco muy profundamente a mi tutor el Ing. Joe Llerena por su dedicación y paciencia, sin sus palabras y correcciones precisas no hubiese podido lograr llegar a esta instancia tan anhelada. Gracias por su guía y todos sus consejos, los llevaré grabados para siempre en la memoria en mi futuro profesional.

Este nuevo logro es gran parte gracias a ustedes; he logrado concluir con éxito un proyecto que en un principio podría parecer tarea titánica e interminable.

Muchas gracias a aquellos seres queridos que siempre aguardo en mi alma

RESUMEN

En la actualidad el rápido crecimiento de la tecnología, así como al auge de las nuevas tendencias de inteligencia artificial, desarrollo de las redes sociales, impulso de la industria 4.0 en general, la globalización, ha venido traer grandes retos en las leyes de protección de datos personales a nivel mundial. El este contexto se multiplican las posibilidades de atentar contra los datos personales de las personas por lo que es imprescindible identificar las nuevas tendencias que facilitan la protección de los datos personales. La presente investigación tiene como objetivo analizar el impacto tecnológico sobre la protección de datos de carácter personal orientada a la infraestructura mediante una revisión literaria. Para cumplir con el objetivo se aplica la metodología PRISMA la cual facilita el análisis de resultados a partir del estudio de referencias de impacto. Se hace una revisión intencionada en Ecuador con el objetivo de que las buenas prácticas identificadas sirvan de guía para mejorar la protección de datos personales de los ecuatorianos que aún lo identifican como una problemática.

Palabras claves: protección de datos personales, seguridad, riesgos, ley, normas

ABSTRACT

Nowadays, the rapid growth of technology, as well as the rise of new trends in artificial intelligence, the development of social networks, the impulse of industry 4.0 in general, and globalization, has brought great challenges to personal data protection laws worldwide. In this context, the possibilities of attacking people's personal data are multiplying, so it is essential to identify the new trends that facilitate the protection of personal data. This research aims to analyses the technological impact on infrastructure-oriented personal data protection by means of a literature review. To meet this objective, the PRISMA methodology is applied, which facilitates the analysis of results based on the study of impact references. An intentional review is carried out in Ecuador with the aim of using the good practices identified as a guide to improve the protection of personal data of Ecuadorians who still identify it as a problem.

Key words: Personal data protection, security, risks, law, rules

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

En la actualidad el rápido crecimiento de la tecnología, así como al auge de las nuevas tendencias de inteligencia artificial, desarrollo de las redes sociales, impulso de la industria 4.0 en general, la globalización, ha venido traer grandes retos en las leyes de protección de datos personales a nivel mundial (Belli and Zingales 2022; López-Chila et al. 2024) El contexto multiplica las posibilidades de atentar contra los datos personales de las personas ya que con el desarrollo de las Tecnologías de la Información (TICs) ha aumentado exponencialmente los datos que se manejan y entre ellos cobran vital importancia los datos personales (Fernández Aller 2012; Wimmer 2022; Tacuri López 2021; Rigchc Mero 2022) Existe una necesidad creciente de establecer mecanismos de protección para prevenir las potenciales violaciones de la seguridad de los datos personales (Ladino, Villa, and López 2011; Vera Navas 2021; Recalde Monar 2021)

Por otra parte, las herramientas de gestión de datos representan un papel fundamental en la sociedad actual, pero a su vez representan grandes riesgos asociados al cumplimiento de leyes y normas de los datos personales. En este sentido (Bravo 2022) afirma que lo ideal sería contemplar desde el diseño de las tecnologías la protección de estos datos, porque sin duda alguna la gobernanza de los datos seguirá siendo un área en constante desarrollo (Muñoz Campuzano 2021; Miranda Jiménez 2021; Moncayo Ronquillo 2021).

Tras el análisis de los diversos ordenamientos y manejos en la infraestructura sostenemos que es cada vez más notorio el requerimiento de independizar la protección de datos y convertirla en una máxima seguridad a la infraestructura (Jácome et al. 2021; Coello Ochoa 2021; Toala Indio 2021).

La mayoría de la información global en mensajes, datos y estructuras en servidores se transmite a través de redes de datos, lo que la expone a posibles ataques cibernéticos. Existen diversas formas en que se puede afectar a los sistemas de transmisión y redes, así como individuos malintencionados (hackers) cuya intención es dañar los sistemas de información. Con el avance de los sistemas informáticos, las conexiones de red, el hardware y el software, se han mejorado los conceptos relacionados con la seguridad. De igual forma se han desarrollado técnicas para hacer que los sistemas de seguridad sean más robustos y en ese sentido, más confiables. No obstante, los programas malignos (malware) evolucionaron, así como también lo hicieron sus creadores (Abid and Jemili 2020).

Cuando se refiere a protección de datos personales los autores han hecho diversos aportes. Según (Fernández Aller 2012) se refiere al derecho fundamental que tiene una persona a controlar el uso que le da a su propia información sea personal o pública, así como los derechos que este individuo puede conceder a un tercero de disponer de esta información.

La Organización de Estados Americanos (OEA), describe los datos personales como la información que permite identificar a una persona, indirecta o directamente. Una identificación está compuesta por datos personales como el número de identificación que es único para cada persona, género, fisiología, economía, aspectos culturales, sociales y factores específicos relacionados a su identidad física y fisiológica. A partir del desarrollo de aplicaciones informáticas y el uso no autorizado de usar los datos personales de las personas los gobiernos han puesto en vigencia leyes que protegen estos datos. Por ejemplo, en Alemania desde el 2008 se crea un derecho constitucional a la confidencialidad e integridad de los sistemas de tecnologías de la información, haciendo énfasis en la necesidad de proteger la información que se maneja en ordenadores personales conectados, celulares, dispositivos inteligentes entre otros (Gupta et al. 2020).

Ecuador es otro país donde se reconoce la necesidad de continuar desarrollando investigaciones en aras de lograr una mayor protección de datos personales en diferentes entornos (Vera Saltos and Vivero 2019; Álvarez 2017; Martínez et al. 2022; Zerega-Prado and Llerena-Izquierdo 2022)

La presente investigación pretende realizar un análisis de los elementos principales que conllevan a la protección de datos, ya que el hecho de que los datos personales sean tratados por terceras personas conlleva un peligro, en el que se juegan aspectos de carácter legal y ético. Se realiza un estudio de la LODP ecuatoriana de manera tal que contribuya a la identificación de riesgos y acciones para fortalecer la seguridad y privacidad de los datos personales de la empresa Courier logística. La investigación tiene como objetivo principal analizar el impacto tecnológico sobre la protección de datos de carácter personal orientada a la infraestructura mediante una revisión de literatura aplicando la metodología prisma para obtener un mapeo sistemático de los principales aportes existentes y llegar a resultados.

2. REVISIÓN DE LITERATURA

Con el auge de las tecnologías una de las principales preocupaciones de los internautas a nivel internacional es la protección de sus datos personales que se encuentran en cualquier lugar del ciberespacio (Cheng and Lai 2012). Incluso la privacidad de la información se trata de forma diferente en el ciberespacio según los distintos tipos de información o entidades, la tendencia general son las medidas preventivas.

Con el desarrollo de los E-Gobiernos en diferentes países se han creado mecanismos para realizar evaluaciones del impacto sobre la intimidad para valorar el impacto de la tecnología de la información sobre la intimidad de la información privacidad de la información (Enríquez 2022)

En investigación realizada por (Abid and Jemili 2020) hace alusión sobre riesgos de datos desprotegidos, gestión inadecuada de permisos y contraseñas, y sobre la base de una muestra de 130 empresas, en la que se analizaron 6.200 millones de archivos, se analizan además mil millones de archivos, algunos datos interesantes relacionados con la seguridad son los siguientes:

- El 21% de las compañías no protegen sus datos
- El 41% de las empresas tiene más de 1000 archivos confidenciales abiertos a cualquier externo.
- El 65% de las empresas tienen más de 500 empleados cuyas contraseñas nunca caducan.

Los datos demuestran que en la actualidad existen disímiles negligencias con respecto a la protección de los datos que son de carácter personal.

Computación en la nube y su relación con la protección de datos

El concepto de computación en la nube (*cloud computing*) se introducido para lograr mayor acceso, interacción y respaldo de la información para las personas, instituciones, gobiernos, etc. Una nube es tipo un sistema paralelo distribuido que contiene un grupo de ordenadores conectados y virtualizados (Buyya et al. 2009; Calero Manueles 2021) Los recursos de los modelos basados en la nube están disponibles a través de internet en cualquier lugar del mundo en centros de datos y clústeres situados en cualquier país. Los recursos informáticos asociados al conceptos son propiedad y están gestionado por quién provee el servicio (Cheng and Lai 2012).

Esta tecnología en los últimos años ha aumentado su utilización por las múltiples ventajas que ofrece entre ellas el autoservicio, el amplio acceso a la red, la agrupación y reserva de recursos, así como su rapidez (Alcívar-Cruz and Llerena-Izquierdo 2023)(Salazar Guzmán 2021)(Reinoso Ordóñez 2021)(Montalvo and Morán 2012). Adicionalmente la computación en la nube ofrece distintos niveles de servicios como son la infraestructura como servicio y la plataforma, la primera ofrece beneficios como el alquiler de espacio de alojamiento y el segundo el despliegue de aplicaciones. Uno de sus grandes beneficios son los costos, los consumidores de estos servicios pagan al consumir el mismo no tienen necesidad de invertir en equipos de cómputo y el mismo tiene gran capacidad de almacenamiento. Las diferentes modalidades de servicios condicionan la seguridad de los datos personales (Rosero Tejada 2021; Robles Balaz 2021; Soto Eras 2021).

El cliente es el responsable de los datos personales que se suben a la nube, en cambio es el proveedor quien tiene el poder para su uso. Según (Fernández Aller 2012) esta tecnología ofrece numerosas ventajas pero a su vez un gran número de riegos sobre los datos personales, la misma tiene implementado mecanismos de respaldos continuos y los datos se pueden alojar en países desconocidos para el cliente. Una de las ventajas que ofrece este servicio está dada por el hecho que quienes proveen servicios en la nube se libraran de la piratería por copia no autorizada lo cual ha sido un problema para los desarrolladores de software por años, en este sentido se ha vuelto más fácil proteger la propiedad intelectual.

Las múltiples ventajas de este servicio pueden a su vez convertirse en desventajas cuando se trata de proteger los datos. Según (Catteddu 2010) el acceso remoto, la virtualización, la falta de control de los datos, el uso masivo de servicios e infraestructuras a terceros, entre otros pueden convertirse en una gran lista de riesgos para la LOPD. La infraestructura de nube es muy susceptible de sufrir ataques maliciosos por parte de externos, personal interno o usuarios de computación en nube. Puede presentar problemas de seguridad con respecto a la integridad de los datos, los controles de cifrado y descifrado y la seguridad de los pagos en la nube (Adejo et al. 2018). A continuación, se mencionan algunas de las problemáticas asociadas al tema.

Al encontrarse los datos en internet se asumen todos los problemas de seguridad asociados a internet como por ejemplo los ataques piratas. Por otra parte, los datos sensibles de las personas como sus historiales médicos ya no están en una cuarentena física. Según (Ristenpart et al. 2009) los riesgos fundamentales surgen al compartir infraestructura física entre usuarios.

Otro importante problema está asociado a que los datos pueden estar alojados en cualquier país y las normativas y regulaciones cambien según su ubicación geográfica. Muchas personas se preocupan por la utilización de sus datos personales con otros fines entre los que se puede encontrar el espionaje gubernamental. Al respecto (Jaeger, Lin, and Grimes 2008) menciona algunos elementos claves como la identificación de los clientes, las actualizaciones automáticas silenciosas y la ausencia total de lanzamientos visibles de productos, facilitan la labor del gobierno en comparación con los mecanismos tradicionales.

Las entidades que proveen servicios en la nube deben elevar su confiabilidad, así como tener claros los términos legales que protejan los datos de carácter personal a los cuales se puede hacer referencias en los contratos. Una alternativa de solución para la protección de datos es realizar transferencias internacionales a países que puedan ofrecer niveles adecuados de protección. Estos mecanismos están autorizados si se conoce el país destino de los datos y las entidades que lo reciben.

En la investigación desarrollada por (Adejo et al. 2018) se resalta con principal preocupación la seguridad y la protección de los datos de los alumnos en la nube como uno de los principales retos para la implantación y el uso del m-learning (Valverde-Macias and Llerena-Izquierdo 2022). En la investigación se propone un marco detallado sobre la seguridad de datos con el fin de disminuir la vulnerabilidad. Dentro de los retos identifica:

- Autentificación: Consiste en proponer una solución CAPTCHA de dos niveles que ayudare a detectar un usuario ilegítimo del legítimo, así como distinguir un programa informático de un usuario humano, el sistema debe ser capaz de verificar la identidad y las credenciales.
- Encriptación de datos: Permite transformar los datos en un código indescifrable antes de almacenarlos y durante la conexión a otras redes. Utiliza parámetros o claves para llevar a cabo la transformación y puede utilizarse para crear una firma digital que permita autenticar fácilmente al usuario. No sólo ayuda a los alumnos o a los proveedores de red, sino también a comprobar los ataques internos a la infraestructura de la nube. Para cifrar los distintos archivos del sistema pueden utilizarse algoritmos de cifrado tradicionales como el Data Encryption Standard (DES), el algoritmo Triple DES (3DES), el algoritmo RSA (clave pública), el Symmetric Key Encryption, el Advanced Encryption Standard (AES) y el algoritmo Blowfish entre otros.
- Autorización y control: Permite controlar la accesibilidad a recursos o servicios en la infraestructura de nube. Se utiliza para determinar si el usuario tiene el privilegio y el

derecho a acceder y realizar una acción determinada. Esto incluye garantizar el control de acceso basado en roles.

- Protección como servicio: Consiste en proporcionar un mecanismo de protección para arquitecturas de sistemas que funcionan en la nube de forma que se prevenga la aparición de ataques y se favorezca la detección temprana de intrusiones/ataques.

Con respecto al impacto tecnológico de la ley de protección de datos de carácter personal la computación en la nube es en la actualidad vista como una infraestructura de servicios donde hay que realizar múltiples investigaciones para garantizar la seguridad de los datos.

Propuestas de soluciones para garantizar seguridad y privacidad

Para solucionar algunas de las dificultades antes mencionadas uno de los mecanismos más fáciles para los usuarios es cifrar los datos que van a poner en la nube, aunque tiene como deficiencia el alto costo del cálculo de los cifrados, además es engorrosa la búsqueda de datos (Cheng and Lai 2012).

Otras propuestas de medidas de seguridad son extender las medidas de control sobre la nube mediante técnicas criptográficas aplicadas (Chow et al. 2009). En el caso de (Pearson, Shen, and Mowbray 2009) proponen un gestor de privacidad y un conjunto de protocolos de seguridad para garantizar la privacidad y el cumplimiento legal.

Otro mecanismo existente son los sistemas de auditoría o evaluación para verificar la privacidad de los datos y su integridad (Wang et al. 2010). Un ejemplo es la existencia de un autenticador homomórfico basado en clave pública e integrándolo con autenticadores aleatorios.

Existen implementaciones exitosas en la rendición de cuentas como lo que se expone en la investigación de (Chen and Wang 2010) donde el servicio de rendición de cuentas introducido puede imponer el cumplimiento a los proveedores de servicios, que participa en colaboraciones empresariales en la nube y los fallos siempre pueden vincularse a sus causantes.

(Pearson and Charlesworth 2009) también propone un enfoque en el que se diseñan soluciones técnicas y de procedimiento para demostrar la responsabilidad como vía para resolver los riesgos jurisdiccionales de privacidad y seguridad dentro de la nube.

Según (Silva and Vale 2021) dentro las técnicas que se pueden aplicar para ganar en la seguridad de los datos en sentido general se encuentran:

- El uso de cortafuegos: Son importantes dispositivos de seguridad que protegen la red bloqueando el tráfico no deseado basándose en políticas de filtrado. Este componente suele situarse en la frontera entre dos redes.
- Sistemas de detección de intrusos (IDS): Permiten monitorizar el flujo de la red para identificar y alertar ataques.
- Sistemas de prevención de intrusos (IPS): Estos son capaces de denegar el acceso al tráfico hostil mientras que el tráfico legítimo sigue teniendo acceso
- Análisis de vulnerabilidades: Es un proceso de prueba rápida en el que se utilizan técnicas o herramientas para identificar posibles vulnerabilidades.
- Aplicación de las normas ISO 27001 y 27002

Por otra parte (Pearson 2009) propone el uso de evaluaciones de impacto sobre la privacidad, este es un mecanismo que apoya a las organizaciones a evaluar el impacto de sus operaciones sobre la privacidad personal, puesto en marcha por la Oficina del Comisario de Información del Reino Unido (ICO). El mismo autor propone principios básicos distintos requisitos de privacidad en las diferentes fases del diseño del software independiente de la tecnología de uso.

Según (Alhadeff, Van Alsenoy, and Dumortier 2012) para proteger los datos de carácter personal es importante considerar los siguientes elementos:

- Compromiso de la organización a la que pertenece la persona con la rendición de cuentas y adopción de políticas internas que adopten la protección de acuerdo con regulaciones.
- Mecanismos internos que pongan en práctica las políticas de protección a la privacidad, incluidas herramientas, formación y educación.
- Sistemas de supervisión interna continua y revisiones de garantía, y verificación del exterior.

La seguridad es un mecanismo o herramienta que se dispone para la protección de datos de carácter personal. En internet se necesitan características muy específicas de seguridad lo que provoca una mayor atención de quienes consumen sus servicios atendiendo las vulnerabilidades que puede ofrecer el sistema (Wimmer 2022).

Entre las medidas que propone (Fernández Aller 2012) se encuentran: llevar registros de incidencia, establecer medidas de control de acceso, sistemas de identificación y autenticación y cautelas en la transmisión de datos.

En la investigación desarrollada por (Alén-Savikko et al. 2020) hace alusión a la importancia de diseñar ciudades inteligentes en contextos seguros donde las personas pueden tener niveles de confianza en los dispositivos inteligentes que se encuentren en sus hogares y la correcta utilización de los datos que se captan desde estos dispositivos.

La protección de los datos personales en las ciudades inteligentes es uno de los mayores retos (Gupta et al. 2020). En el entorno actual dentro de las recomendaciones que se realizan en la investigación se encuentra la necesidad de proteger el anonimato en los datos que se registran y la aplicación de mecanismos de privacidad para proteger a las personas.

De manera similar en la investigación desarrollada por (Ducuing 2020) identifica la protección de los datos personales como un riesgo potencial en la gobernanza de datos. El autor hace una discusión en base a cómo los datos personales se convierten en motivos de competencias empresariales y gana el que mayor monopolio da datos tiene, lo que a su vez permite ganar tomar decisiones que conllevan a un crecimiento económico.

En (Silva and Vale 2021) se realiza una propuesta de metodología basada en la ley brasileña de protección de datos personales (Ley Nº 13.709/2018) de manera que esta sea referencia para la construcción de infraestructuras de redes informáticas. Esta propuesta se basa en tres fases fundamentales, en primer lugar, se crea un modelo de seguridad que incluye el uso de herramientas como Firewall e IDPS con el propósito de formar una defensa sólida a nivel arquitectónico. En la segunda, se aplican herramientas enfocadas en el análisis de vulnerabilidades para encontrar fallas que pongan la red y por último se generaran informes de las vulnerabilidades y se aplican las contramedidas (técnicas y herramientas) recomendadas. El trabajo constituye una opción viable para aplicar en las empresas brasileñas.

Los retos se multiplican en la misma medida en la que avanza la ciencia. En la investigación realizada por (Williams et al. 2021) aprovechan los conceptos clave de la ciencia de la resiliencia para avanzar en la ingeniería de seguridad de sistemas de próxima generación para describir mejor las complejidades, el dinamismo y la no linealidad observados en el rendimiento de la seguridad. El autor presenta un modelo de red multicapa y un modelo modificado de cadena de Markov en tiempo continuo que capta explícitamente las interdependencias en la ingeniería de seguridad de sistemas. Los resultados muestran cómo las métricas basadas en redes pueden incorporar conceptos de resistencia a las métricas de rendimiento para la ingeniería de seguridad de sistemas de próxima generación aplicable para datos personales.

En la investigación realizada por (Sheng et al. 2020) también se presenta una propuesta de avanzada con un método de predicción de la situación de seguridad basado en el algoritmo de optimización de enjambre de partículas y la red neuronal de memoria a largo-corto plazo para los eventos de seguridad de la red en el plano de datos SDN. Se utiliza la información estadística del incidente de seguridad en el proceso de jerarquía analítica para calcular el valor de riesgo de la situación de seguridad del plano de datos SDN. Para validar la investigación se utilizan datos históricos del valor de riesgo de la situación de seguridad para construir un modelo de predicción de red neuronal artificial. Al final se utiliza un modelo de predicción para prever el futuro valor de riesgo de la situación de seguridad de los datos de índole personal. Los experimentos demuestran que este método tiene una buena precisión de predicción y estabilidad.

Dentro de los principales retos que se asocian a la Ley de protección de datos personales se identifica a grandes rasgos tres importantes retos:

- Los derechos de los individuos en relación con los beneficios de la sociedad en que vive, ¿hasta qué punto puede mantener una persona sus datos en total privacidad, si estos datos afectan el desarrollo social y democrático? (Fernández Aller 2012)
- Transparencia con los sistemas, los individuos no conocen qué se hace con los datos personales que se introducen en los sistemas fundamentalmente los que están de cara a internet (Belli and Zingales 2022).
- No se abarcan las tecnologías disruptivas de las IoT en normas y leyes lo cual introduce una amplia exposición a amenazas y vulnerabilidades (Gupta et al. 2020)

Norma ISO 27701

Como se ha mencionado hoy en día a partir del desarrollo tecnológico en todas las organizaciones se manejan un número considerable de información y en gran medida relacionadas con la información personal de las personas. Se procesa información relacionada con la identificación personal y esta va en aumento por día. La protección de esta información se ha convertido en una creciente necesidad de la sociedad por que se legisle y regule de manera específica en cualquier parte del mundo. Se hace imprescindible la actualización de mecanismos vigentes para la protección de datos personales, así como la adopción de estándares personales que protejan a los individuos (Ladino, Villa, and López 2011).

El Sistema de Gestión de la Seguridad de la Información (SGSI) definido en la norma ISO/IEC 27001 permite que se añadan y relacionen los requisitos de un sector específico, tal como el sector de las empresas que realizan Courier en el país, esto para que no sea necesario que se cree un nuevo sistema de gestión. La norma contempla tantos requisitos técnicos y a la vez requisitos operativos necesarios que van a reducir las vulnerabilidades respecto a la protección de datos personales. En ella se ha definido un proceso de inicio a fin en el que están bien definidas cuatro etapas que van desde planificar, implementar, monitorear y mejorar continuamente el sistema.

Bajo lo que indica esta norma, también se facilita la orientación, dirección y especificación al momento que se requiere realizar una evaluación de impacto de para la protección de datos de índole personal en cualquier entidad, definiendo en el informe las medidas adoptadas para gestionar y mitigar riesgos. La estructura de la norma pasa por varias secciones entre las que se incluyen el abordaje a las políticas definidas para el respaldo de la información, una gestión adecuada de riesgos, la seguridad en los sistemas, un adecuado control de acceso de usuarios, el reporte y gestión de incidentes.

Las organizaciones que adopten esta norma y cumpla con sus requisitos generará pruebas documentales de cómo gestiona la información de índole personal. Además, que está el hecho de que los socios comerciales pueden sentirse más confiados en llegar a un acuerdo comercial al conocer el tratamiento que se da a la información y cómo se la protege.

Entre los controles más importantes que establece la norma se encuentra: Políticas para salvaguardar la información, seguridad de la organización, seguridad del recurso humano, administración adecuada de activos, criptografía, seguridad física, control de accesos y seguridad que tiene que ver con el entorno, seguridad en las operaciones diarias, seguridad en las comunicaciones, administración adecuada de incidentes, información de la seguridad de aspectos de la gestión empresarial.

La norma propone un conjunto de buenas prácticas donde se resalta el hecho de que la información debe ser transparente en todo el proceso, así como su comunicación, también trata sobre el derecho a acceder a la información y los posibles casos en los que se debe aplicar la limitación, rectificación, oposición o suprimir este derecho. La portabilidad de la información es trata también. Se establecen procesos de notificación de violaciones a la seguridad de la información, por ejemplo, cuando se identifica una violación a la seguridad de los datos, se debe notificar a la autoridad de control.

Las instituciones deben hacer un esfuerzo por capacitarse, aplicar y certificarse en esta norma la cual protege eficazmente la seguridad informática, reduce cualquier amenaza cibernética y guarda un alto nivel de coherencia. La desventaja de aplicación de la norma radica en sus altos costos para empresas de menor tamaño o con recursos más limitados (Ladino, Villa, and López 2011).

También se sugiere la aplicación de otras normas internacionales como la ISO 31000 e IEC 31010 que resultan eficaces en cualquier tipo de organización que requiera evaluar el impacto que surge luego de implementar controles y herramientas para la protección de datos. También se refieren otras normas como la ISO/IEC 27017:2015 en donde se trata sobre las diferentes tecnologías de la información y de las técnicas de seguridad, los buenos códigos de prácticas para establecer controles de seguridad adecuados para la información. La ISO/IEC 27002 se enfoca en servicios en la nube y la ISO/IEC 27018: 2020 en nubes públicas.

Ley orgánica establecida para la proteger datos de índole personal en Ecuador

A partir de preocupaciones existentes por parte de investigadores y ecuatorianos en general de la inexistencia de mecanismos regulatorios asociados a la cultura de proteger los datos de índole personal se acrecienta la necesidad de impulsar en el país este tema. En el 2017 en la legislación vigente el término "hacker" no estaba clasificado en el marco penal, cual contribuía a la existencia de una brecha tanto legal como tecnológica en el ámbito de la protección de datos personales (Álvarez 2017).

Adicionalmente se identificaban carencias fundamentalmente en el entorno empresarial lo cual puede afectar la integridad de las personas La ambigua situación de la preservación de los datos personales en el Ecuador es la principal motivación de (Vera Saltos and Vivero 2019) en un estudio realizado donde enfoca sus análisis en la protección de datos personales por parte de las empresas.

Dentro de los acontecimientos relevantes en Ecuador se puede hacer mención la afectación ocurrida en el 2019 en la cual la empresa israelí vpnMentor dio a conocer que alrededor de 20 millones de datos de ecuatorianos se vulneraron debido a fallas de seguridad de la empresa ecuatoriana empresa ecuatoriana Novaestrat. Entre los datos vulnerados se encuentra datos de tipo crediticio y otros, lo que ha expuesto a las personas a que se sean vulnerables a que su identidad sea robada, así como fraude financiero. A partir de este incidente el presidente en curso, presentó en el 2017 un proyecto de ley ante la asamblea para proteger los datos de índole personal, el cual requería de la colaboración tanto de entidades públicas como del sector

privado, así como de ayuda nacional e internacional. En el 2021 este proyecto de ley fue aprobado y entró en rigor en el 2021. Esta ley otorga a las empresas privadas y entidades públicas un plazo de dos años para iniciar los procesos internos de adaptación (Arcos-Argudo, Matute-Pinos, and Fernández-Mora 2023).

Pese al plazo establecido para su introducción, han existido deficiencias para su aplicación en el marco empresarial. Las principales causas están enfocadas a desconocimiento y falta de compromiso de los actores principales. Las empresas recopilan información personal en varios procesos para el funcionamiento de su negocio, sin embargo, muchas veces no se considera que esta información y su procesamiento deben cumplir con las regulaciones legales establecidas por la LOPDP en cuanto a manejo, procesamiento, almacenamiento, uso de bases de datos, tecnología y seguridad (Arcos-Argudo, Matute-Pinos, and Fernández-Mora 2023).

La LOPDP establece como principio fundamental el derecho por parte de los titulares de los datos, además de regular el proceso de transferencia de datos internacionalmente, mientras dispone el tratamiento de datos sensibles. La ley recoge el derecho del titular de conocer acerca de cómo se procesan sus datos, así como el acceso a ellos en todo momento, de acuerdo con los principios de transparencia y lealtad. En lo relacionado con el ámbito material la LOPD aplica a los datos contenidos en cualquier soporte, pero no aplica, pero aplica al tratamiento de datos domésticos lo cual es una insuficiencia (Martínez et al. 2022)

No se puede establecer una comparación entre la LOPD de Ecuador y la norma ISO 27101 pues ambas herramientas se complementan. La norma propone un conjunto de buenas prácticas para para reducir el riesgo de vulnerabilidades respecto a la protección de datos personales, mientras que la ley desde su estructura contempla la política de seguridad de la información en todo el documento. Por otra parte, el cumplimiento de la ley contribuye a la gestión de riesgos con la protección de datos de índole personal y garantiza el control de acceso en diferentes capítulos. La introducción de la ley en la práctica garantiza la seguridad de la información en los sistemas y la administración adecuada de incidentes. La ley surge posteriormente a la norma ISO y su base legal recoge las buenas prácticas que esta propone.

En la tabla 1 se establece a través de una matriz la relación entre los capítulos de la LOPD y las secciones que contiene la Norma ISO 27101, como se observa, los capítulos de la ley tienen asociación con alguna de las buenas prácticas de la norma.

Tabla 1 Relación entre la Norma ISO 27101 y la LOPD

Capítulos LOPD	Norma ISO 27				
	Salvaguardar la información	Administrar riesgos	Controlar el acceso	Seguridad de software	Administración de incidentes
Datos especiales	x		x		
Comunicación, transferencia y acceso a datos de índole personal por terceros		x			x
Seguridad de datos de índole personal	x	x	x	x	
Autoridad de protección de datos personales	x	x			

Según (Arcos-Argudo, Matute-Pinos, and Fernández-Mora 2023) en el país se carece de medidas adecuadas para llevar a cabo un peritaje efectivo que facilite identificar a los ciberdelincuentes.

A partir de las problemáticas existentes en Ecuador, (Arcos-Argudo, Matute-Pinos, and Fernández-Mora 2023), propone una serie de puntos clave que se deben considerar para mejorar en el país la protección de los datos personales, entre ellos se encuentran: (1) identificar claramente el rol del de la empresa como responsable o encargado, (2) definir el responsable de Protección de Datos personales que se encargará internamente y capacitarlo, (3) establecer medidas de seguridad básica y también establecer en cada una de esas actividades de tratamiento de los datos personales y por último (4) identificar las bases legales para cada actividad de tratamiento.

En la investigación realizada por (Jácome et al. 2021) justifica la necesidad de que en Ecuador también exista el cargo de "Delegado de Protección de Datos", existente ya en muchas partes del mundo fundamentalmente en el reglamento europeo. En los países latinoamericanos surge la inquietud de las funciones que puede cumplir el encargado y cómo su puesto puede contribuir al monitoreo y control de la protección de datos de índole personal.

3. METODOLOGÍA

La metodología incluye una revisión sistemática de bases de datos académicas, análisis de artículos claves, se organiza la información de manera estructurada para ofrecer una visión completa y objetiva de la investigación existente.

Adicionalmente, se realiza un análisis detallado de las referencias, identificando tendencias y resultados claves. Finalmente, se sintetiza la información para crear una visión coherente del impacto tecnológico sobre la protección de datos de índole personal, se identifican los principales riesgos asociados y los desafíos para trabajos fututos. Para el desarrollo de la investigación se utilizan las bases teóricas de la metodología PRISMA, que permite responder a los objetivos propuestos en la investigación.

El estudio requiere que se haga una revisión exhaustiva acerca de la literatura existente. La revisión sistemática permite ampliar el cúmulo de conocimientos acerca del tema tratado, identificando tendencias en las investigaciones previas realizadas con el fin de tener una amplia visión de la problemática y así mismo de las posibles soluciones.

Para desarrollar la revisión se realiza una revisión de la literatura la cual apunta a fuentes a una revisión exploratorias, utilizando fuentes secundarias de información halladas en bases indexadas de las cuales se extrajo artículos de relevancia. Se describe el objeto de estudio de la investigación lo cual permite reducir la investigación a los trabajos relacionados con el área. Se realizan las siguientes tareas:

1. Definición de pregunta de investigación, alcance de la revisión, lo que incluye la descripción de las bases de datos revisadas y las cadenas de texto utilizadas
2. Definición de los criterios de exclusión y selección de artículos
3. Selección de trabajos primarios (En las bases de datos seleccionadas)
4. Definición de criterios de análisis
5. Sintetizan los resultados
6. Grafican los hallazgos
7. Análisis de resultados

Definiciones para la búsqueda

En este trabajo, las palabras claves en la investigación fueron: "Protección de datos personales", "Ley de Protección de datos personales", "Seguridad y protección de datos personales","Norma ISO 27101", En el ámbito de esta investigación la mayor bibliografía consultada fue en idioma inglés.

Preguntas de investigación para la obtención de resultados

RQ1: ¿Cuáles han sido los principales problemas asociados a la protección de datos personales?

RQ2: ¿Cuáles son los principales riesgos asociados a la protección de datos personales?

RQ3: ¿Qué incidencia tienen las leyes y normas de protección de datos personales para las personas e instituciones?

Criterios de inclusión y exclusión:

Se consideraron los siguientes:

- El artículo debe tener relación con el objetivo de la investigación.
- Se evaluaron trabajos en el idioma inglés fundamentalmente y español.
- Se excluyen artículos cuyo objeto de investigación no esté bien definido o apunte hacia otro enfoque.
- Se excluyen artículos con un mal diseño de investigación, o cuyos resultados se basen en opiniones de expertos, también aquellos donde no se han planteado al menos una pregunta de investigación, así como tesis o artículos que no estuviesen indexados en bases de datos reconocidas.

Alcance de la revisión

Este estudio se ha centrado fundamentalmente en las bases de datos: Web of Science, IEEE Xplore, ScienceDirect y ACM.

El período de búsqueda incluye publicaciones desde el 2008 hasta la actualidad

Las cadenas de búsquedas utilizadas para encontrar publicaciones fueron fundamentalmente:

- (personal data protection AND personal data protection law AND risks to the protection of personal data AND difficulties)
- TITLE ((“personal data protection” OR “good practices for data protection” OR “personal data protection infrastructure services” OR “risks to the protection of personal data”) AND (“trends” OR “applications”)

Estas cadenas se ajustaron a los propios formatos de cada base de datos.

Conducta de búsqueda:

La variedad de la investigación implica una búsqueda de fuentes bibliográficas y se agrupa en dos rondas.

En la primera ronda, se realizó tres iteraciones de cribado y filtrado para determinar los estudios relacionados con la protección de los datos de índole personal. En la primera iteración se eliminaron los duplicados. A continuación, se eliminaron todos los artículos no relacionados con la protección o seguridad de datos personales investigando los títulos y resúmenes. Por último, en la segunda iteración se realizó una revisión intensiva de los artículos completos. Las tres iteraciones utilizaron criterios de elegibilidad similares. En la segunda ronda, se realizó una única iteración de cribado y filtrado basada en el proceso inteligente para todos los artículos obtenidos en la iteración de la primera ronda. Posteriormente, el conjunto final incluido estaba relacionado con la protección de los datos de índole personal y las leyes y normas asociados al objeto de estudio.

4. RESULTADOS

En el presente epígrafe se presentan los resultados obtenidos luego de aplicar la metodología PRISMA para realizar una revisión de la literatura con mayor profundidad. Se identificaron en una primera búsqueda un total de 1520, tras examinar el título y resumen se excluyeron de este total 1100 quedando un total de 420 para otra ronda de revisión. Del total de 420 fueron descartados 300 artículos entre las principales causas de la decantación se encontraron artículos duplicados, tesis no publicadas y artículos que solo se pudo encontrar el resumen. A partir de la revisión de 120 artículos en fase de elegibilidad se vuelven a decantar un total de 90 artículos luego de hacer una revisión de texto completo y dentro de las principales causas se encontraron, artículos publicados en otros idiomas que no eran ni español ni inglés, artículos que no aportaban directamente a la investigación, investigaciones envejecidas entre otros. Quedaron finalmente para realizar el estudio un total de 30 artículos elegibles. En la figura 1 se muestra el proceso de selección de artículos aplicando la metodología PRISMA.

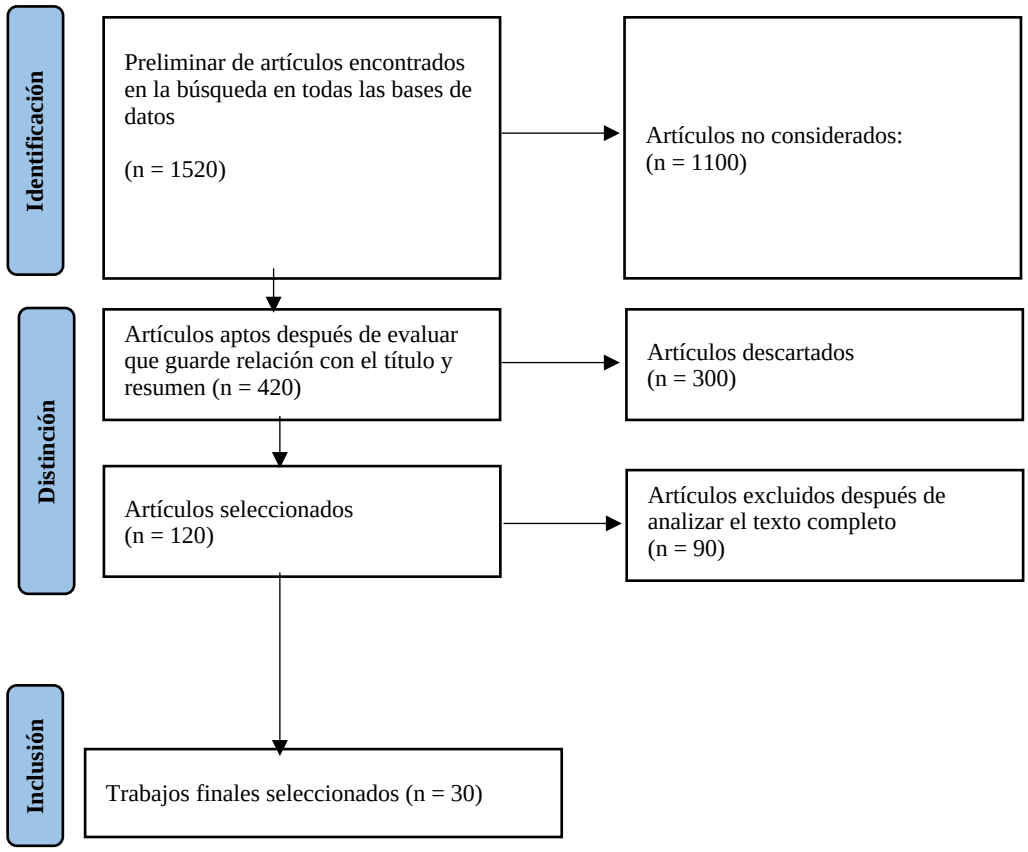


Figura 1 Estudios identificados bajo el modelo PRISMA

Del total de 30 trabajos revisados se obtiene un total de 19 trabajos de la base de datos de IEEExplore, 3 trabajos en Springer, 2 de la Web of Science y 6 de Scopus. Se eliminaron trabajos duplicados, así como no relacionados directamente con el objetivo de la investigación.

Figura 2 Distribución por años de la bibliografía

Como se muestra en la figura 2 el estudio de las referencias fue a partir del año 2008. El mayor número de referencias analizadas fue a partir del 2019 lo cual tiene correspondencia con el desarrollo que ha tenido el objeto de estudio en los últimos años. La mayor parte de las referencias sin de los últimos diez años, se puede concluir respecto que existe actualidad de las referencias y un balance apropiado. La búsqueda realizada arrojó trabajos actualizados a nivel internacional fundamentalmente en Europa y se hizo espacial énfasis en la búsqueda de resultados en Ecuador. es un tema novedoso que aún tiene mucho campo por investigar.

En la figura 3 se muestra las principales temáticas que arrojaron las búsquedas en la investigación.

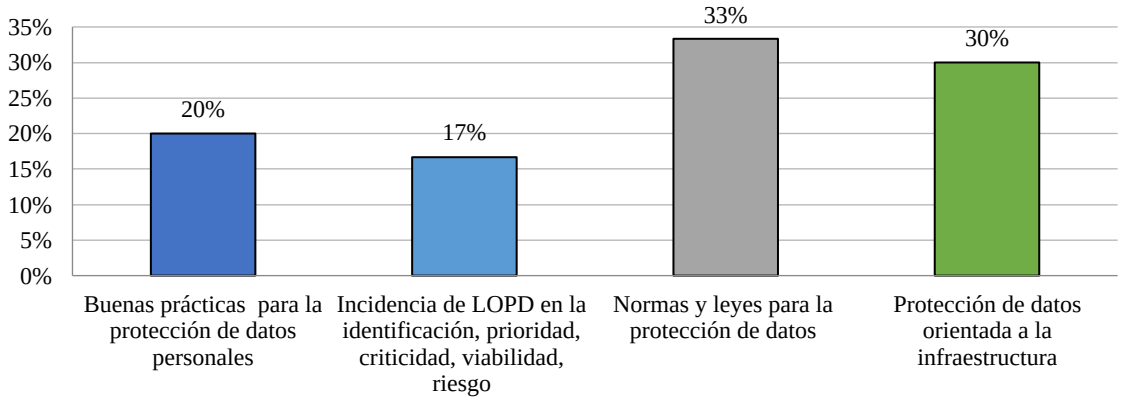


Figura 3 Temáticas abordadas en la revisión

En la figura 3, el 33% de las referencias analizadas están enfocadas a las normas y leyes para la protección de datos personales. El 30% de las investigaciones estuvo orientado a la protección de los datos personales enfocados a la infraestructura de servicios computacionales, en donde se hace énfasis en el almacenamiento de datos (nube). El 20 % de los estudios analizados estaban relacionados con buenas prácticas que se deben seguir para la protección de los datos y el 17% de los trabajos tocaba temas relacionados con la incidencia de las leyes de protección de datos en la identificación, prioridad, criticidad, viabilidad y riesgos de los datos personales. En sentido general hubo un balance en análisis de referencias y se identificaron diversos puntos comunes en todos los estudios como la necesidad de incrementar la protección y seguridad de datos personales a través de diversos mecanismos, leyes, normativas, entre otras.
A partir del estudio de las 30 referencias analizadas en la investigación se identifican criterios que se repiten en las investigaciones y que constituyen puntos de atención para la protección y seguridad de los datos personales. Se muestran en la figura 4.

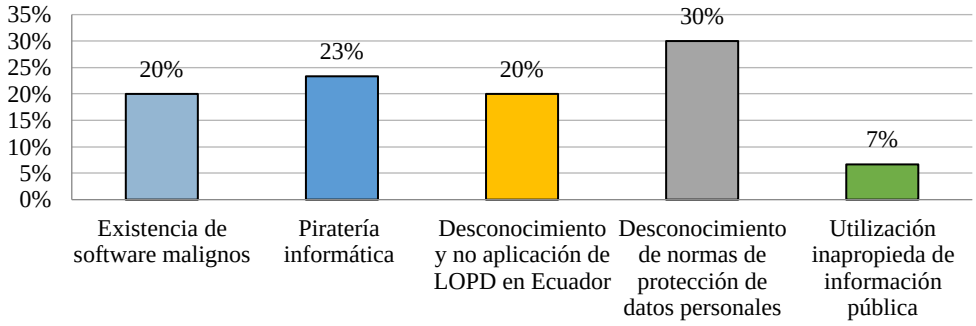


Figura 4 Criterios que se repiten en las investigaciones

En la Figura 4 el 30% de las investigaciones hacen referencia al desconocimiento de normas asociadas a la protección de datos por parte de las personas naturales, así como por parte de empresas e instituciones en general. Al existir desconocimientos de las normas y leyes, la aplicación de buenas prácticas no se hace efectiva lo cual aumenta el número de irregularidades asociadas al objeto de estudio.
El 23% y el 20% de las investigaciones menciona dentro de sus problemáticas la existencia de piratería informática y software malignos en el mismo orden que afectan la integridad de la información de las personas y pueden causar problemas desde el punto de vista económico y social no solo para las personas sino también para las instituciones.

En el caso específico de Ecuador a pesar de la existencia de la ley de protección de datos el 20% de las investigaciones reflejan que aún esta no tiene aplicación en muchos ámbitos laborales y personales asociado fundamentalmente al desconocimiento de los acápites de la ley, así como analfabetismo digital.

Por el último el 7% de las investigaciones hacen referencia a que existe un uso inapropiado de la información pública que los usuarios ponen en diferentes espacios lo cual constituye una importante vulnerabilidad en la protección y seguridad de los datos, estos pueden usarse para otros fines de lucro.

En la Figura 5, las principales limitaciones identificadas asociadas a la protección de datos desde el punto de vista tecnológico.

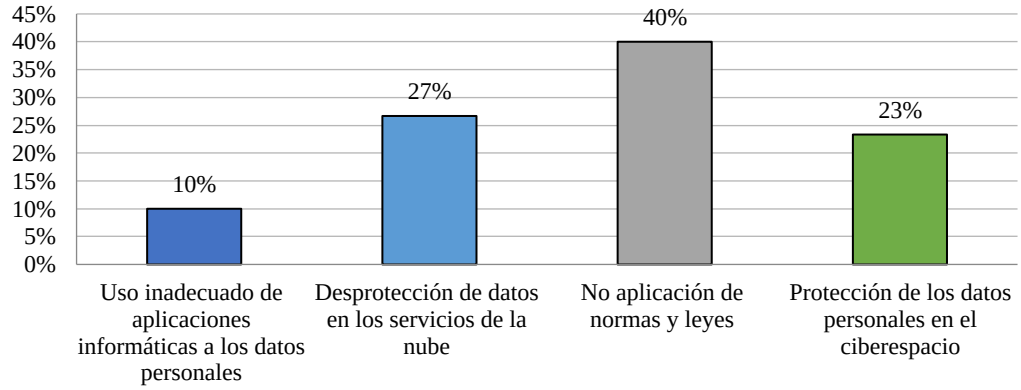


Figura 5 principales limitaciones identificadas asociadas a la protección de datos desde el punto de vista tecnológico

Como se observa en la Figura 5 el mayor porciento de 40% corresponde a la no aplicación de normas de referencia en la protección de datos personales como la ISO 27101 y las leyes de protección de datos trae consigo en primer lugar que no se consideren las buenas prácticas para la concepción de ecosistemas digitales y posteriormente la no aplicación de leyes provoca que se incurran en ilegalidades y no se apliquen medidas de sanción.

En el 27% de las investigaciones se hacen referencia a la desprotección de los datos personales en los servicios que se ofrecen en la nube lo cual es una importante tendencia a nivel mundial desde el punto de vista de infraestructura, esta incidencia afecta a un número considerable de personas a nivel internacional y requiere de la atención de investigadores y gobiernos. El 23% hace referencia a la protección de datos en el ciberespacio en sentido general este indicador se incrementa con el desarrollo de la industria 4.0, así como la preocupación de los usuarios. Por último, el 10% hace alusión a un uso inadecuado de aplicaciones informáticas donde se

introducen datos personales sin protección lo cual provoca la captura de información desde estas aplicaciones.

Por otra parte, a partir de las de la revisión de las referencias se identifican las mayores tendencias en propuestas de soluciones antes las problemáticas identificadas. En la Figura 6 se muestran los principales temas en las propuestas de solución.

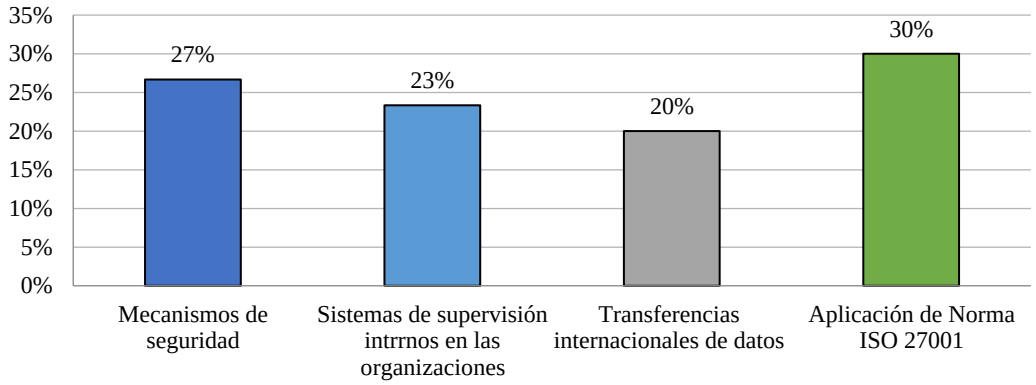


Figura 6 Principales propuestas de soluciones

En la Figura 6 se presentan las principales tendencias de soluciones ante las problemáticas antes identificadas. El 30% de las investigaciones hacen referencia a la necesidad de adoptar las buenas prácticas que se recomiendan en la Norma ISO 27001 como pilar de referencia a nivel internacional en la protección de datos. Los gobiernos e instituciones que apliquen las buenas prácticas recomendadas tienen una parte del éxito. El 27% de los autores reconoce que establecer mecanismos de seguridad para la protección de datos personales es fundamental para ganar en confianza de estos, se hace énfasis en la importancia de hacerlo desde la propia concepción de los diseños de soluciones tecnológicas. El 23% de los trabajos hace referencia de la importancia de contar con sistemas internos de supervisión en las organizaciones e instituciones de manera que se detecten las vulnerabilidades y se identifiquen los riesgos de manera preventiva lo cual facilite la protección y seguridad de los datos personales. Por último, el 23% de las investigaciones encentran en las trasferencias internacionales de datos una vía de respaldo a la protección de datos, esta solución es viable siempre que los países destino cuenten con regulaciones que protejan los datos personales.

Finalmente, en la Figura 7 se presentan los principales retos asociados al objetivo de la investigación.

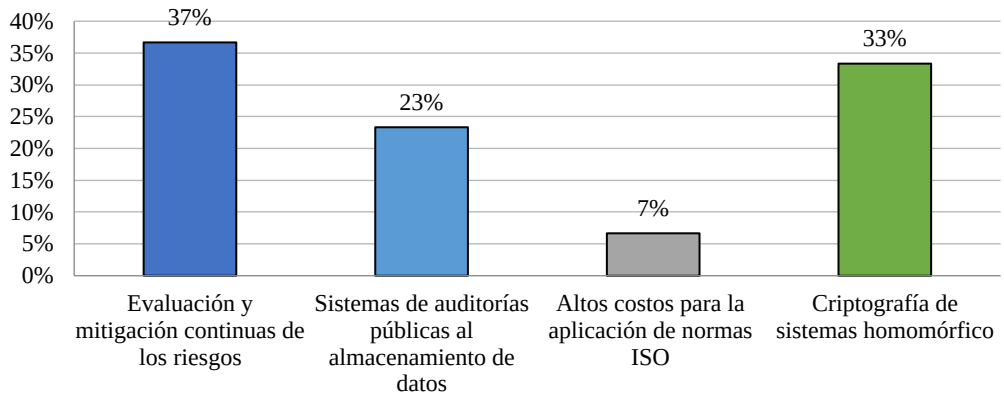


Figura 7 Principales retos asociados a la protección de datos

Como se muestra en la Figura 7 el principal reto identificado por los autores con el 37% está asociado a la evaluación y mitigación continúa de los riesgos asociados a la protección de datos. Si los riesgos no son identificados no se elaboran planes de acciones y se crean nuevas herramientas y mecanismos para enfrentar los problemas asociados a la protección y seguridad de datos. El 33% identifica la criptografía como una herramienta útil y aplicable pero que necesariamente debe seguir evolucionando desde el punto de visto innovador de manera tal que pueda enfrentar con mayor eficiencia los problemas actuales. El 23% hace alusión a la necesidad de instaurar auditorías públicas a los servicios y aplicaciones que ofrecen almacenamiento de datos como por ejemplo la nube, esto contribuiría en gran medida a un mayor control y protección de los datos. Por último, el 7% hace referencia que los altos costos para la aplicación de Normas como la ISO 27001, constituyen un resto para las empresas e instituciones con menor grado de recursos, por lo que es importante que en cada país existan y se apliquen leyes y mecanismos que contribuyan a la protección de datos personales.

A partir del estudio realizado en la investigación se identifican un conjunto de riesgos potenciales asociados a la protección de datos personales. En la tabla se realiza una matriz de incidencia de riesgos potenciales identificados y el cubrimiento que pueden tener estos riesgos en la Ley de Protección de Datos. Estos riesgos pueden a su vez desglosarse para un mayor plan de acciones.

Tabla 2 Matriz de identificación de riesgos

No	**Riesgos identificados**	Salvaguardar la información	Administrar riesgos	Controlar el acceso	Seguridad de software	Administración de incidentes
1	Cuentas de correos expiradas	x	x	x		x

2	Robos de correspondencia de información personal	x		x		x
3	Ataques internos de una institución o empresa				x	x
4	Utilización inapropiada de información pública	x		x	x	x
5	Robo de tarjetas personales digitales a través de dispositivos de lectura de datos.	x		x		
6	Programas informáticos malignos			x	x	x
7	Piratería informática (hacking)	x		x	x	x
8	Uso de buscadores web para obtener identidad					x
9	Servicios de Internet basados en contenidos creados por el usuario como las redes sociales	x				
10	Robo de identidad	x			x	x
11	Analfabetismo digital	x				x
12	No inclusión desde el diseño de las aplicaciones la protección de datos					x
13	Captura de datos a través de dispositivos del internet de las cosas					

A partir de la Tabla 2 la mayor parte de los riesgos identificados tiene un nivel de incidencia en la ley de protección de datos. Queda por cubrir los riesgos asociados a la captura de datos a través de dispositivos de IoT que no está contemplado en la ley. Al ser este impacto tecnológico de auge a nivel internacional debe intensional el trabajo en este importante apartado.

5. DISCUSIÓN

Para dar cumplimiento el objetivo de la investigación se analizaron un total de 30 referencias bibliográficas con actualidad científica. A partir del estudio se identificaron elementos importantes para la investigación tales como las principales dificultades asociadas a la protección de datos personales a nivel internacional. De igual manera se identificaron las principales tendencias en la protección de datos y las normas de referencia que sirven de guía para empresas e instituciones. Se identificaron las principales propuestas de solución antes las vulnerabilidades que pueden existir en la protección y seguridad. El tema tiene grandes perspectivas en todos los sectores de la sociedad, la comunidad científica debe continuar trabajando para incrementar los resultados de aplicación en el mundo.

En el caso específico de Ecuador a pesar de estar vigente una ley asociada a la protección de datos personales aún esta no ha sido aplicada a gran escala y se detectan vulnerabilidad en diferentes ámbitos. Los riesgos identificados pueden tomarse como una lista de chequeo para la empresa ecuatoriana Courie.

6. CONCLUSIÓN

Se realiza una revisión literaria a profundidad a partir de la metodología PRISMA, la cual facilita una revisión detallada de la temática cumpliendo el principal objetivo de la investigación. Se identificaron un total de 1520 trabajos relacionados con la temática en las diferentes bases de datos y finalmente siguiendo la metodología se analizaron a profundidad 30 trabajos los cuales evidencian el impacto tecnológico sobre la protección de datos de índole personal orientada a la infraestructura

A partir del estudio se determina que alcance de incidencia de la ley de protección de datos es a nivel internacional, desde diversos ámbitos gubernamentales, empresariales y personales. La identificación de riesgos asociados a la protección de datos personales puede tributar considerablemente a la disminución de ataques, así como la aplicación de buenas prácticas siguiendo estándares internacionales como la Norma ISO 27001.

A partir del estudio de trabajos relacionados se identificaron un conjunto de riesgos potenciales que se repiten en las investigaciones de los autores y pueden ser generalizados. La ley de protección de datos de índole personal ampara la incidencia de la mayoría de los riesgos, pero los mismos deben ser correctamente tratados escenarios específicos. Es un tema novedoso que tiene múltiples campos de explotación en el futuro por el alto impacto tecnológico que existe y la utilización de los datos personales con diversos fines.

REFERENCIAS

Abid, Ahlem, and Farah Jemili. 2020. “Intrusion Detection Based on Graph Oriented Big Data Analytics.” *Procedia Computer Science* 176: 572–81. https://doi.org/10.1016/j.procs.2020.08.059.

Adejo, Olugbenga W, Isaiah Ewuzie, Abel Usoro, and Thomas Connolly. 2018. “E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure.” *International Journal of Information Technology and Computer Science (IJITCS)* 10 (4): 1–9. https://doi.org/10.5815/ijitcs.2018.04.01.

Alcívar-Cruz, Bruno, and Joe Llerena-Izquierdo. 2023. “After-Sales and Customer Loyalty Strategies for Fixed Internet Through the Implementation of Virtual Assistance in the Ecuadorian Context.” In *Intelligent Technologies: Design and Applications for Society*, edited by Vladimir Robles-Bykbaev, Josefa Mula, and Gilberto Reynoso-Meza, 139–49. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-24327-1_12.

Alén-Savikko, Anette, Shakila Bu-Pasha, Heidi Himmanen, Päivi Korpisaari, Sara Lehtilä, and Juha Vesala. 2020. “Personal Data Protection, Frequency Regulation and Competition Law in the Context of Smart City Infrastructure.” In *Oikeuksia, Vapauksia Ja Rajoituksia: Viestintäoikeuden Vuosikirja 2019*. Helsingin yliopisto. https://doi.org/10.1080/13600834.2023.2208992.

Alhadeff, Joseph, Brendan Van Alsenoy, and Jos Dumortier. 2012. “The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions.” In *Managing Privacy through Accountability*, 49–82. Springer. https://doi.org/10.1057/9781137032225_4.

Álvarez, Luis Enríquez. 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.” *Foro: Revista de Derecho*, no. 27: 43–61. https://doi.org/1390-2466.

Arcos-Argudo, Miguel, Karina Matute-Pinos, and Mesías Fernández-Mora. 2023. “Análisis Comparativo de La Ley Orgánica de Protección de Datos Personales Del Ecuador Con La Legislación Colombiana Desde Un Enfoque de Ciberseguridad y Delitos Informáticos.” *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E60: 100–114. https://doi.org/10.7238/idp.v0i33.376365.

Belli, Luca, and Nicolo Zingales. 2022. “Data Protection and Artificial Intelligence Inequalities and Regulations in Latin America.” *Computer Law & Security Review* 47: 105761. https://doi.org/10.1016/j.clsr.2022.105761.

Bravo, Fabio. 2022. “Data Management Tools and Privacy by Design and by Default.” *Privacy and Data Protection in Software Services*, 85–95. https://doi.org/10.1007/978-981-16-3049-1_8.

Buyya, Rajkumar, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. 2009. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility.” *Future Generation Computer Systems* 25 (6): 599–616. https://doi.org/10.1016/j.future.2008.12.001.

Calero Manueles, Elvis Fabian. 2021. “Aplicación Móvil Para Reconocimiento de Texto Sobre Carnés Estudiantiles Utilizando Visión Por Computadora Basada En La Nube.” 2021. http://dspace.ups.edu.ec/handle/123456789/20902.

Catteddu, Daniele. 2010. “Cloud Computing: Benefits, Risks and Recommendations for Information Security.” In *Web Application Security: Iberic Web Application Security Conference, IBWAS 2009, Madrid, Spain, December 10-11, 2009. Revised Selected Papers*, 17. Springer. https://doi.org/10.1007/978-3-642-16120-9_9.

Chen, Shiping, and Chen Wang. 2010. “Accountability as a Service for the Cloud: From Concept to Implementation with BPEL.” In *2010 6th World Congress on Services*. https://doi.org/10.1109/SERVICES.2010.79.

Cheng, Fa-Chang, and Wen-Hsing Lai. 2012. “The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy.” *Procedia Engineering* 29: 241–51. https://doi.org/https://doi.org/10.1016/j.proeng.2011.12.701.

Chow, Richard, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. 2009. “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control.” In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, 85–90. https://doi.org/10.1145/1655008.1655020.

Coello Ochoa, Ingrid Nicole. 2021. “Análisis de Ciberataques En Organizaciones Públicas Del Ecuador y Sus Impactos Administrativos.” 2021. http://dspace.ups.edu.ec/handle/123456789/20738.

Ducuing, Charlotte. 2020. “Data as Infrastructure? A Study of Data Sharing Legal Regimes.” *Competition and Regulation in Network Industries* 21 (2): 124–42. https://doi.org/10.1177/1783591719895390.

Enríquez, Alberto. 2022. “Gobierno Digital: Pieza Clave Para La Consolidación de Estados Democráticos En Los Países Del SICA,” March.

Fernández Aller, Maria Celia. 2012. “Algunos Retos de La Protección de Datos En La Sociedad Del Conocimiento. Especial Detenimiento En La Computación En La Nube (Cloud Computing).” *RDUNED. Revista de Derecho UNED*, no. 10: 125–45.

Gupta, Maanak, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. 2020. “Security and Privacy in Smart Farming: Challenges and Opportunities.” *IEEE Access* 8: 34564–84. https://doi.org/10.1109/ACCESS.2020.2975142.

Jácome, Tannia Cecilia Mayorga, Joe Luis Carrión Jumbo, Álvaro Gabriel Benítez Bravo, and Henry Rodrigo Vivanco Herrera. 2021. “The ‘Delegate of Data Protection’: Strategic Planning in Information Security Case Ecuador.” In *Journal of Physics: Conference Series*, 1993:12040. IOP Publishing. https://doi.org/10.1088/1742-6596/1993/1/012040.

Jaeger, Paul T, Jimmy Lin, and Justin M Grimes. 2008. “Cloud Computing and Information Policy: Computing in a Policy Cloud?” *Journal of Information Technology & Politics* 5 (3): 269–83. https://doi.org/10.1080/19331680802425479.

Ladino, Martha Isabel, Paula Andrea Villa, and Ana María López. 2011. “Fundamentos de ISO 27001 y Su Aplicación En Las Empresas.” *Scientia et Technica* 17 (47): 334–39. https://doi.org/10.7238/idp.v0i33.376366.

López-Chila, Roberto, Joe Llerena-Izquierdo, Nicolás Sumba-Nacipucha, and Jorge Cueva-Estrada. 2024. “Artificial Intelligence in Higher Education: An Analysis of Existing Bibliometrics.” *Education Sciences* 14 (1). https://doi.org/10.3390/educsci14010047.

Martínez, Mario Ramiro Aguilar, Julio Alfredo Paredes López, Diego Patricio Gordillo Cevallos, and Gabriela Paulina León Burgos. 2022. “La Protección de Datos Personales En Ecuador.” *Estudios Del Desarrollo Social: Cuba y América Latina* 10 (especial 1). https://doi.org/2308-0131.

Miranda Jiménez, Joan Noheli. 2021. “Mapeo Sistemático de Metodologías de Seguridad de La Información Para El Control de La Gestión de Riesgos Informáticos.” 2021. http://dspace.ups.edu.ec/handle/123456789/20966.

Moncayo Ronquillo, Karol Cristina. 2021. “Seguridades de La Información Bases de Datos Distribuidas: Un Mapeo Sistemático.” 2021. http://dspace.ups.edu.ec/handle/123456789/21701.

Montalvo, Andrés, and Paúl Morán. 2012. “Propuesta de Un Sistema de Gestión Del Conocimiento Para El Departamento de Tecnología de La Información y La Incidencia Económica Para El Grupo MAVESA.” 2012. https://dspace.ups.edu.ec/handle/123456789/3653.

Muñoz Campuzano, Peter Steeven. 2021. “Modelos de Seguridad Para Prevenir Riesgos de Ataques

Informáticos: Una Revisión Sistemática." 2021. http://dspace.ups.edu.ec/handle/123456789/20932.

Pearson, Siani. 2009. "Taking Account of Privacy When Designing Cloud Computing Services." In *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 44–52. IEEE. https://doi.org/10.1109/CLOUD.2009.5071532.

Pearson, Siani, and Andrew Charlesworth. 2009. "Accountability as a Way Forward for Privacy Protection in the Cloud." In *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1*, 131–44. Springer. https://doi.org/10.1007/978-3-642-10665-1_12.

Pearson, Siani, Yun Shen, and Miranda Mowbray. 2009. "A Privacy Manager for Cloud Computing." In *Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1*, 90–106. Springer. https://doi.org/10.1007/978-3-642-10665-1_9.

Recalde Monar, John Angelo. 2021. "El Ciberacoso Por Redes Sociales En El Ecuador." 2021. http://dspace.ups.edu.ec/handle/123456789/20945.

Reinoso Ordóñez, Luigi Andrés. 2021. "Desarrollo de Sistema Informático Para La Gestión de Pagos de Cuotas de Los Residentes de La Urbanización Belo Horizonte." 2021. https://dspace.ups.edu.ec/handle/123456789/20332.

Rigchc Mero, Andrea. 2022. "Determinación de Los Peligros En Las Redes Sociales En Entorno a Niños y Adolescentes Para Uso y Prevención." 2022. http://dspace.ups.edu.ec/handle/123456789/22843.

Ristenpart, Thomas, Eran Tromer, Hovav Shacham, and Stefan Savage. 2009. "Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds." In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 199–212. https://doi.org/10.1145/1653662.1653687.

Robles Balaz, Gissell Johanna. 2021. "Desarrollo de La Aplicación Web Para El Registro de Matrículas y Gestión de Conducta e Incidencias En La Escuela José Martí." 2021. http://dspace.ups.edu.ec/handle/123456789/20951.

Rosero Tejada, Luis Fernando. 2021. "El Phishing Como Riesgo Informático, Técnicas y Prevención En Los Canales Electrónicos: Un Mapeo Sistemático."

Salazar Guzmán, Byron Jordan. 2021. "Desarrollo de Una Aplicación Bajo Android Para El Control y Monitoreo de Unidades Vehiculares En La Empresa TCPLUMESAL SA." 2021.

Sheng, Mingren, Hongri Liu, Xu Yang, Wei Wang, Junheng Huang, and Bailing Wang. 2020. "Network Security Situation Prediction in Software Defined Networking Data Plane." In *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, 475–79. IEEE. https://doi.org/10.1109/AEECA49918.2020.9213592.

Silva, Luis Castro, and Samyr Vale. 2021. "A Methodology for Network Security Infrastructure According to the New Brazilian General Law for Personal Data Protection." *International Journal of Computer Applications* 183 (07): 2021. https://doi.org/10.5121/ijnsa.2020.12502.

Soto Eras, Wilmer Moisés. 2021. "Desarrollo Del Portal Web de La Fundación Nuestra Señora Del Cisne Para La Gestión de Servicios En El Cantón Durán." 2021. http://dspace.ups.edu.ec/handle/123456789/20947.

Tacuri López, Ingrid Lilibeth. 2021. "Acoso Por Medio de Las Tecnologías En Las Redes Sociales Durante Tiempos de Pandemia En Ecuador, Una Revisión Sistemática." 2021. http://dspace.ups.edu.ec/handle/123456789/20242.

Toala Indio, Yomar Isidoro. 2021. "Delitos Informáticos Frecuentes En El Ecuador: Casos de Estudio."

Valverde-Macias, Alejandra, and Joe Llerena-Izquierdo. 2022. “Google Classroom as a Mobile and Blended Learning Strategy for Salesian Groups Training.” In *Communication, Smart Technologies and Innovation for Society*, edited by Álvaro Rocha, Paulo Carlos López-López, and Juan Pablo Salgado-Guerrero, 97–106. Singapore: Springer Singapore. https://doi.org/https://doi.org/10.1007/978-981-16-4126-8_10.

Vera Navas, Nelson Alexander. 2021. “Modelo de Seguridad Informática Para Riesgos de Robo de Información Por El Uso de Las Redes Sociales.” 2021. http://dspace.ups.edu.ec/handle/123456789/20949.

Vera Saltos, María Alejandra, and Belen Vivero. 2019. “¿ Vida Privada O Muerte a La Privacidad?: Protección De Datos Personales En La Relación Empresa-Cliente En Ecuador (Private Life or Death to Privacy?: Data Protection in Ecuador).” *Protección De Datos Personales En La Relación Empresa-Cliente En Ecuador (Private Life or Death to Privacy*. https://doi.org/10.2139/ssrn.3538879.

Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. 2010. “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.” In *2010 Proceedings Ieee Infocom*, 1–9. Ieee. https://doi.org/10.1109/INFCOM.2010.5462173.

Williams, Adam D, Thomas Adams, Jamie Wingo, Gabriel C Birch, Susan A Caskey, Elizabeth S Fleming, and Thushara Gunda. 2021. “Resilience-Based Performance Measures for Next-Generation Systems Security Engineering.” In *2021 International Carnahan Conference on Security Technology (ICCST)*, 1–5. IEEE. https://doi.org/10.1109/ICCST49569.2021.9717388.

Wimmer, Miriam. 2022. “Foreword: Advancements and Challenges for Latin American AI and Data Governance.” *Computer Law & Security Review* 47: 105759. https://doi.org/10.1016/j.clsr.2022.105759.

Zerega-Prado, José, and Joe Llerena-Izquierdo. 2022. “Arquitectura de Consolidación de La Información Para Seguros de La Salud Mediante Big Data.” *Memoria Investigaciones En Ingeniería* 0 (23 SE-Artículos). https://doi.org/10.36561/ING.23.3.