UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
Análisis de brechas para la protección de datos personales en base a LOPD caso Mobilvendor
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)
Autora:
ARCOS QUISPE MARIA GABRIELA
Tutor:
MSc PABLO M RECALDE V

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde V. con C.I: 171168505-5 en mi calidad de Tutor del proyecto de investigación titulado: Análisis de brechas para la protección de datos personales en la empresa Mobilvendor en base a LOPD

Elaborado por: María Gabriela Arcos Quispe de C.I: 1725532582 estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

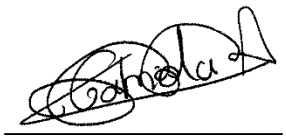
Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, María Gabriela Arcos Quispe con C.I: 1725532582, autor/a del proyecto de titulación denominado: Análisis de brechas para la protección de datos personales en la empresa Mobilvendor en base a LOPD. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023



Firma

orcid: 0000-0001-5781-9349

Tabla de contenidos

Índice de tabla

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Según Rodríguez et al, (2020) a finales del siglo XIX aparece el comercio electrónico y con esto nacen transacciones como órdenes de compras, pagos de servicio, entre otras operaciones que interactúan tanto empresa como cliente sin tener un control rígido sobre la información que se manipula.

Con el paso del tiempo estas transacciones fueron ganando terreno en el ámbito comercial y con la llegada del internet el mundo de las ventas se globalizó y esto ha generado que los mercados evolucionan cada vez de una forma distinta. Según un estudio realizado en Ecuador el 82,3% por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) de Mipymes utilizan Internet. De acuerdo a la encuesta realizada muestra un porcentaje de: microempresas 48,6%, medianas 56,9% y pequeñas 52,9%, dando un total general de 52,8%. Cabe señalar que, a pesar del acceso que tienen a Internet el uso se concentra enviar correos y la realización de tareas administrativas, solo un 27% de las Mipymes tiene presencia en la web. (MINTEL, 2020).

Según Roldan, (2021) con el pasar del tiempo el uso de nuevas plataformas tecnológicas y una inminente globalización de los datos sensibles de un individuo, se vuelve más fácil encontrar vulnerabilidades que afectan la privacidad de las personas y dar perjuicio a los consumidores o clientes, por lo expuesto se hace imperativo trabajar en un derecho autónomo, ya que pocos países han logrado darle proceso y tratamiento, con esto dimensionar la falta de desarrollo, son 194 los países oficialmente reconocidos por la ONU, de los cuales tan solo 120 han incorporado legislación referente a la protección de datos.

Toda esta información personal puede estar almacenada digitalmente que por lo general el gobierno y entidades financieras tiene bajo su protección, es por esto por lo que es necesario proteger el derecho a la privacidad, esto quiere decir que los datos serán manipulados bajo consentimiento del involucrado.

Según Enríquez L., (2021), en el país ya se aplica la Ley Orgánica de Protección de Datos Personales (LOPD), que regula cómo las organizaciones nacionales y extranjeras dan tratamiento, proceso, seguimiento, conservación y explotación comercial de los datos. Con el apoyo de esta ley se pretende garantizar el cumplimiento de un estándar mínimo, para poder ser considerado como un país confiable para la traspaso y manejo de información personal, esto brinda un mecanismo para el crecimiento de las empresas ecuatorianas. En Ecuador, la LOPD entro en vigencia y fue publicada el 26 de mayo del 2021. Desde la publicación de esta

ley todas las empresas públicas y privadas cuentan con un tiempo de adaptación de dos años, para que todos sus procesos sean en base a esta nueva normativa.

Una de las actividades de gran alcance a nivel nacional e internación es la venta de bienes de consumo masivo, el movimiento derivado de la venta de estos productos se puede detectar en los sistemas de comercialización. (Cabezas, 2018)

La adquisición de productos de consumo masivo en Ecuador según (Coba, 2021) ha sufrido un incremento en gasto en el primer bimestre del 2021, donde creció un 9% el equivalente a USD 81 millones frente al mismo período del 2020.

Es por esto, por lo que la investigación se ha centrado en un nicho fundamental en las empresas de distribución masiva, estas empresas al tener un crecimiento significativo tienen una amplia base de información acerca de sus clientes, ya que constantemente estas distribuidoras requieren obtener un detalle específico de sus clientes para poder ofertar de mejor manera los productos.

Este segmento comercial tiene la obligación de dar fiel cumplimiento de la ley, para evitar demandas, o sanciones.

Por tanto, debe basarse en un sistema que proteja los datos, asegure el correcto y legal tratamiento de los mismos, estos sistemas deben tener como objetivo asegurar la privacidad y manejo de los datos del titular de acuerdo a los procesos de cada cliente.

Problema de investigación

Ecuador al tener una infraestructura tecnológica en desarrollo y un mercado informal muy arraigado en sus consumidores, la aplicación de la LOPD, fue aprobada el 26 de mayo del 2021 empieza a ser un problema, que dejará en evidencia a varias empresas que trabajan almacenando datos o transacciones con ellos de forma masiva.

El consumidor ecuatoriano aún se resiste al uso de plataformas tecnológicas, pero con la llegada de la pandemia a mundo entero, en estos dos años se ven cambios significativos al uso de estas, sin embargo, existe resistencia a entregar información personal por canales digitales, es de esperar que el uso de esos mismos canales tecnológicos al estar controlados o regidos por una nueva ley pueda causar desconocimiento o incluso problemas legales entre empresa y consumidor.

Es importante comprender que este cambio de carácter obligatorio puede llegar a ser muy tortuoso para una organización que no haya tomado las debidas precauciones legales sobre la nueva ley.

La empresa «Mobilvendor» es una plataforma que transaccionan con aproximadamente 700 empresas de distribución de productos de primera necesidad a nivel nacional y es necesario garantizar que el flujo de información cumpla con los distintos estándares requeridos por la LOPD, por lo que se ve en la obligación de garantizar a sus clientes que la información personal con la que trabaja cuente con todas las autorizaciones que solicita la ley.

Actualmente Mobilvendor no cuenta con una guía de aplicación para el LOPD, por lo que el enfoque de esta investigación pretende generar un campo más claro sobre los ajustes que debe realizar la organización en su oferta de servicios para llegar a cumplir con las exigencias de la ley.

¿Cómo proteger los datos personales en las empresas tecnológicas del tipo desarrollo de software según lo expuesto en la Ley Orgánica de Datos Personales?

Objetivo general

Realizar un análisis de brechas respecto al uso y manejo de los datos personales que mantiene la empresa «Mobilvendor» respecto a la ley de protección de datos personales de Ecuador.

Objetivos específicos

- Identificar mecanismos mediante un cuadro comparativo que tiene actualmente la empresa Mobilvendor para cumplir con la LOPD.
- Realizar un análisis de cumplimiento de los procesos actuales para el amparo de datos personales en base a lo establecido en la LOPD.
- Generar guía con las mejores recomendaciones sobre el manejo de información acorde al LOPD y dejar bases para un correcto manejo de seguridad informática para comunidades sostenibles.

Vinculación con la sociedad y beneficiarios directos:

El presente trabajo investigativo busca ayudar a cada una de las empresas para que puedan adaptar en sus procesos el correcto manejo de los datos personales, esto debido a que está por culminar el periodo de adaptación establecido para esta ley. Para cumplir con esta ley, las empresas grandes y pequeñas se deben adaptar al proceso de innovación en el uso del manejo de los datos entregados.

Con el avance de la tecnología, día a día, la privacidad de las personas se vuelve vulnerable y el mal uso de su información genera incertidumbre, es por esto que todas las personas deben conocer cuáles son sus derechos para proteger sus datos.

De acuerdo a lo observado se brindará asesoría para que las empresas puedan cumplir con los establecido en la ley, dependiendo el servicio que manejen y con este aporte se busca controlar la pérdida de información y con esto evitar que la imagen institucional se devalué.

Esta investigación se centrará en industria, innovación e infraestructura el objetivo número nueve de los objetivos de desarrollo sostenible, que contribuye a métodos de seguridad, para que todas las personas tengan acceso y conocimiento a su información de forma confiable.

Sin embargo, al ser una ley completamente nueva para el Ecuador queda mucho campo por estudiar y que esta ley pueda ser analizada y adaptada bajo los distintos requerimientos internacionales.

Beneficiarios Directos

Mobilvendor: Esta empresa desarrolló un software que presta servicios de control de inventario y fuerza de ventas a empresas del sector de consumo masivo y por ende su base de información de datos es amplia, para esta investigación se considera un beneficiario directo ya que se pretender realizar un análisis de brechas respecto a los procesos que solicita seguir a la ley con lo establecido en la misma.

Sociedad: Se refiere al conjunto de individuos que se relacionan entre sí, se rigen en determinadas normas o reglas, es un beneficiario directo ya que los productos de consumo masivo son nuestro diario vivir y el consumo hace que las distintas distribuidoras contengan datos de sus clientes amplia para poder ofertar servicios.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se presenta la contextualización de la Ley Orgánica de Protección de Datos y la metodología utilizada sobre el proceso de investigación.

1.1. Contextualización general del estado del arte

Los Datos Personales (DP), es cualquier información específica de una persona que permita la identificación de manera clara y específica de un individuo esto se puede presentar por referencia a un número de identificación o varios factores. económicas, culturales, sociales o espirituales. (Colombato, 2021).

La forma de hacer negocios con bienes y servicios ha generado grandes cambios generacionales, superando los medios tradicionales, creando posibilidades tecnológicas utilizando funciones de compraventa que evolucionan incluso con las nuevas tendencias del mercado. La principal oportunidad en estos tiempos modernos es participar en el comercio electrónico, aprovechando la estandarización de la red y su flujo de datos (Meltezer, 2018).

Según La Organización Mundial del Comercio (OMC),la comercialización internacional que es mutable por naturaleza, hoy por hoy se enfrenta a una feroz transformación de innovación tecnológica, con la aplicación constante de la IA se han generado nuevas estructuras de negocios que se reproducen con facilidad por medio de páginas web, aplicaciones y las ya permanentes aplicaciones móviles con sus redes sociales nos han brindado un estado de mayor comunicación y conectividad eliminado las barreras fronterizas tradicionales (OMC, 2018).

La digitalización ha provocado cambios muy importantes en el consumo de información en todos los sectores. Las empresas están expuestas al valor añadido de poseer datos personales y ahora estos pasan a formar parte de su patrimonio, por lo que su correcto manejo se ha convertido en un tema innegable en los últimos años. Incidentes como el mal uso de los datos o violaciones de sus medidas de seguridad amenazan la reputación de las empresas, dando lugar a sanciones por no actuar con responsabilidad, por lo que debe verse desde una perspectiva regulatoria. incluye: legislación, normativa específica del sector y buenas prácticas (Mendoza, 2018).

Según Brunet (2015) hoy, con diversas tecnologías del siglo XXI, todos los datos se almacenan en: servidores de correo electrónico; crm; servidores privados; computadoras portátiles, discos duros portátiles; tabletas o teléfonos móviles de los empleados; tecnología SAS; sitios web; intranets, entre otros.

Estos ejes principales de datos se controlan y supervisan en todos los entornos tecnológicos para hacer cumplir las políticas, estrategias y procedimientos del sistema de gestión de documentos.

En los últimos años han aparecido varias empresas dedicadas a recolectar los DP; claramente con objetivos comerciales. Lo grave de esta situación es la completa falta de seguridades con la que transaccionan estas empresas, las cuales al administrar estos datos ponen en peligro el velo de seguridad de las personas. Por lo que la ley de la que hablamos propone normas de tratamiento con el fin de salvaguardar y prevenir la pérdida de esta valiosa información. (Arellano, 2020)

Los DP forman valiosa información dentro de las organizaciones. Por ello, tienen un alto impacto, en cuanto a la reputación sobre el manejo de este segmento, llegando incluso actualmente a incidir en el crecimiento o caída de grandes multinacionales. (Mendoza, 2018)

Las empresas que fueron creadas con el fin de recopilar datos personales deben tener seguridad en toda su infraestructura ya que pueden llegar a ser atacados y esta información podría caer en manos equivocadas, con en esto no solo las empresas que recopilan datos deben proteger la información, todas las empresas que prestan servicios de sistemas comerciales deben precautelar esta información y entregar a sus clientes las garantías necesarias para precautelar estos datos.

Actualmente, los datos personales tienen un valor económico que se puede comprar con activos intangibles como el software o incluso con el valor comercial de un nombre de dominio, por lo que se ha considerado el petróleo de la sociedad y la información por ser un valor no económico. que estos datos representan, no sobre los datos derivados de sí mismos, sino sobre su procesamiento. (Enríquez, 2018)

Según Roldan, (2021), se está creando conciencia a nivel mundial sobre la formulación de un marco regulatorio para el resguardo y uso adecuado de los datos personales. En el mes de mayo del año 2016, desde el consejo europeo se publica el GDPR, el cual empieza a generar controles por primera vez el 25 de mayo de 2018. Su objetivo principal es fortalecer las normas de protección de datos y actualizar las normativas europeas, lo que condujo directamente a nuevos cambios técnicos.

1.2. Proceso investigativo metodológico

Este proceso de indagación se realizó mediante el enfoque cuantitativo, Según Santa et al, (2017) proporciona una base de contenido que hace referencia a las causas, características, funcionamiento y enriquecimiento de los cambios hipotéticos de solución, que ayudan al crecimiento del conocimiento general.

Investigación Descriptiva:

Según Tamayo (2003) «Comprende lo descriptivo mediante registros, análisis e interpretación, y el proceso de fenómenos, este enfoque se realiza sobre conclusiones dominantes o grupos de personas»

Investigación de Campo

Se realiza una investigación de campo ya que mediante el análisis de brechas se realizó una comparativa de lo que tiene actualmente en la empresa con lo esperado.

Se toma la investigación por campo ya que, al realizar un análisis de brechas, se validará directamente los procesos que maneja actualmente la empresa respecto a los datos personales y los establecidos de acuerdo con el estudio realizado sobre la protección de datos.

Las técnicas de investigación de campo se ejecutan directamente en lugares y personas donde se genera el fenómeno que se estudia. Su principal objetivo es recolectar datos de fuentes directas por medio de un proceso de observación estructurada y aplicar diversas herramientas desarrolladas previamente: estudio de casos, entrevista, encuesta , trabajo práctico de campo, etc. Estas herramientas no funcionan solas, sino que a menudo se combinan con documentos. (Guzmán, 2019)

Investigación Exploratoria

Esta investigación nos da una visión general sobre temas poco conocidos y nos permite identificar fenómenos pocos desconocidos. sí, la investigación exploratoria trata de generar una referencia simple sobre un tema muchas veces desconocido. Entre sus objetivos podemos mencionar la posibilidad de formular un problema de investigación, extrayendo datos y términos que permitan generar las preguntas necesarias (Morales, 2020).

Métodos y técnicas de recolección de la información

Para la recolección de información, mediante la revisión de documentos relacionados a la seguridad de la información que se encuentran establecidos en el sistema.

Mediante observación se pudo identificar en los departamentos como manejan la información de los clientes y se puede identificar si conocen los riesgos sobre los ataques informáticos.

Es importante que en el diseño de la investigación identifiques las estrategias o planes que te llevarán a identificar respuestas a las preguntas planteadas en la investigación, así como las herramientas que te guiarán en la recopilación de esta información, la información relevante debe tomar en cuenta ciertos factores como el diseño a utilizar. (Guzman, 2019).

Para desarrollar este estudio, se hizo a través de investigación bibliográfica y trabajo de campo.

La investigación bibliográfica según Arteaga, (2020) está basada en la recopilación de información de las investigaciones publicadas, en estos recursos se pueden incluir recursos como revistas, libros, informes, también incluye medios electrónicos como grabaciones de sonido, videos, películas y recursos en línea como páginas web.

Los enfoques de investigación cuantitativos y cualitativos son estudiados desde diferentes ángulos, pero lo que ambos tienen en común es el uso de la investigación bibliográfica, solo que este tipo de investigación respalda cada enfoque. (Ocampo, 2019)

En cuanto a la recopilación de información para este estudio, que se realizó en forma electrónica, este estudio tuvo como objetivo principal verificar los procesos que cada empresa debe implementar para proteger datos personales. La ley es nueva en el país, pero algunos países ya han implementado este proceso y tienen información detallada al respecto.

1.3. Análisis de resultados

Para poder verificar los resultados de la investigación se realizó una entrevista a un especialista en la materia de protección de datos: Mg. Alberto Moncayo obteniendo los siguientes resultados:

Mediante la protección de datos se garantiza los derechos fundamentales y la libertad de decisión de quienes otorgaron su información, especialmente su intimidad y honor.

Los consumidores a nivel general están cada vez más concienciados sobre la importancia de mantener sus datos protegidos y es por esto por lo que valoran las empresas que aseguren el tratamiento correcto de los mismos.

Cuando las distintas empresas trabajan y aplican seguridades adecuadas, están trabajando en el bienestar de todos, porque el uso indebido de la información de particulares y empresas pueden causar perjuicios muy graves.

Es por esto que se promulgada la LOPD en Ecuador, y se toman en cuenta los distintos parámetros que deben considerar para el uso y cuidado de datos sensibles, dentro de lo establecido por la ley según Legal Alert, (2021) son las siguientes:

- Obtener el consentimiento del propietario tanto a la recepción como como en el traspaso de datos personales.
- Para un análisis de riesgo, amenazas y vulnerabilidades
- Determinar medidas de seguridad
- Se debe realizar por parte del responsable una evaluación de impacto en el correcto tratamiento de datos.
- Notificar las vulnerabilidades de seguridad hacia los datos personales, en un tiempo máximo de cinco días después de lo ocurrido, a menos que dicha violación constituya una violación o amenaza para los derechos de los individuos.
- El encargado del procesamiento de los datos es responsable de notificar cualquier vulneración al titular en un lapso de dos días.
- La transferencia internacional se debe sustentar en un marco legal que contemple los estándares determinados.
- Se puede realizar transferencias o comunicaciones internacionales de datos

CAPÍTULO II: PROPUESTA

La propuesta del tema de investigación planteada como: Análisis de brechas para la protección de datos personales en base a LOPD caso «Mobilvendor».

2.1 Fundamentos Teóricos Aplicados

Delitos Informáticos

Los delitos informáticos como concepto reconocido internacionalmente se denomina Ciberdelincuencia; previamente debemos comprender que de acuerdo con distintas fuentes de normativa legal nacional y extranjera que este concepto como tal de delito informático no posee una definición exacta. Ya que debido a su extensa variedad de cometer faltas graves a la ley se optó por generalizar a todos estos problemas como “criminalidad de internet” o “delincuencia informática”, adoptando la categoría de delitos informáticos. (Sosa, 2022)

Cuando no existen las respectivas medidas de seguridad y mantenemos información personal registrada en distintos sistemas, puede llegar a ser atacado utilizando los distintos mecanismos de robo de información.

Ley de protección de datos personales

El GDPR ha cambiado el mundo, por eso se ha vuelto popular hoy en día. Lo cierto es que el RGPD responde a un largo desarrollo de más de 40 años resguardando los datos personales de los ciudadanos europeos, que ha afectado a otras regiones del mundo, incluida América Latina. La aplicabilidad directa del RGPD y su alcance extraterritorial implica que todas las instituciones del mundo deben cumplir con sus obligaciones. (Enríquez, 2021)

Las obligaciones a la protección de datos personales descansa sobre tres ejes centrales esenciales: la vigencia del derecho legal respecto al uso, gestión y manipulación de datos personales; que el contenido de estas disposiciones es el establecimiento de límites de tratamiento, los cuales deben incluir ciertas disposiciones sobre los propios datos personales; En última instancia, la finalidad de las normas es proteger a las personas, en el sentido más amplio posible, pero permitiendo o facilitando la autonomía o autodeterminación. (Huerto, 2017)

El procesamiento de DP debe ser diseñado con la finalidad de ayudar a la humanidad. Todo lo relacionado con la LOPD no es un derecho absoluto, al contrario, debe tratarse en un contexto de función social y equilibrado que junto a otros derechos y obligaciones cumplen el principio de proporcionalidad. Este reglamento garantiza todos los derechos, libertades fundamentales y los principios contenidos en la carta y los tratados, en particular las libertades

de la vida privada, la familia, el hogar y la comunicación, la protección de datos, los derechos individuales de los trabajadores, la libertad de pensamiento, de conciencia y de religión, libertad de expresión e información, libertad de empresa, tutela judicial efectiva y derecho a un juicio justo y diversidad cultural, religiosa y lingüística. (Gobierno de España, 2016)

Con las nuevas leyes adaptadas al RGPD, toda Latinoamérica se enfrenta a un incómodo periodo de ajuste. Algunas áreas de la seguridad de la información pueden enfrentar varios desafíos al adaptar los métodos organizacionales para cumplir con las disposiciones de este reglamento. Hay que tener en cuenta que la mayoría de los profesionales en temas de ciberseguridad en América Latina están capacitados y certificados de acuerdo con métodos desarrollados en EE. UU., como EC-COUNCIL, SANS Institute e ISC2. Del mismo modo, las métricas generales en temas de seguridad de la información, como la familia ISO/IEC 27000, adoptan el enfoque anterior al RGPD, pero puede actualizarse en un futuro próximo. Por ello, es fundamental la cooperación de la Unión Europea para desarrollar o adaptar métodos de evaluación de riesgos que puedan adaptarse a las leyes de los países latinoamericanos. (Enriquez, 2021)

Se realizará un breve estudio sobre el sistema de gestión de la seguridad de la información ya que se tomará como base para guiar a la empresa Mobilvendor, mediante el análisis brechas verificar las políticas y controles sobre los riesgos que se encuentra sometida la información.

Información Personal e Internet

Una de los principales temas jurídicos relacionados con la tecnología y el derecho es cómo Internet influye en el derecho fundamental a la protección de DP. Debido al profundo impacto de los desarrollos tecnológicos en la determinación de las configuraciones de este derecho fundamental, se ha llamado la atención, con carácter previo a su análisis, a la evolución normativa del tratamiento que tiene la protección de los datos personales recibidos en Europa y en su defecto, la recepción y configurando leyes dentro de nuestro ordenamiento jurídico. (Guerrero, 2020)

El entorno social de la comunicación e información exponen necesariamente en el centro de atención a los individuos; es decir, abordar la comunicación desde una perspectiva de “derechos” que incluye anteponer la dignidad, el desarrollo humano y los derechos de ciudadanía digital y global, a partir de consideraciones tecnológicas o de la relación entre fabricante y consumidor. (Gregorio y Ornelas, 2011)

Principios Básicos de la LOPD

Según Porcelli, (2019) la información personal se han convertido en el eje central de las organizaciones y con el objetivo de llevar un control eficiente en la gobernanza de datos pero sin descuidar las obligaciones que tienen las empresas con los clientes, se plantean normas generales de LOPD, que constan de estándares regulares, en el cual se exponen su aplicación al tratamiento de D.P. iniciando el capítulo II que identifican los principios básicos que deben regir al tratamiento, los cuales son: legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, compromiso, seguridad y confidencialidad y responsabilidad proactiva.

Con respecto al principio de legitimación, el artículo once, enumera una serie de supuestos según los cuales, el responsable está habilitado al tratamiento de los datos:

1) El titular autoriza el uso de su información para determinadas acciones que serán notificadas o expuestas previamente.
2) La autorización de ser necesario podrá ser usada para fines legales siempre que sea justificada ante una autoridad competente;
3) En un proceso de defensa en el que se de tentativa de vulnerabilidad de los derechos que tiene un titular.
4) Cuando se trate de una obligación legal en el que el titular sea parte;
5) Para el cumplimiento de una obligación legal aplicable al responsable;
6) Siempre que exista un interés vital del titular o de otra persona;
7) Por razones en determinado de fuerza mayor en el que exista un interés mediático alto
8) En el caso de que se vean violentados los derechos de un tercero en especial al tratarse de niños o adolescentes y considerando que los derechos del titular no se vean comprometidos.

Cuando se trabajen sobre procesos en el que se deba obtener la aceptación previa del titular el artículo doce, determina las condiciones para que dicho consentimiento sea válido.

Responsable del tratamiento de Datos

Como garantía de dar fiel cumplimiento a lo solicitado por la ley, la nueva persona es el delegado de protección de datos, cuya función es informar y asesorar al encargado de los requisitos exigidos en la normativa, además, debe velar por la supervisión y cooperación, con las autoridades de la organización, se debe crear un registro nacional de DP, el cual los administradores a través de la autoridad deben actualizar constantemente. (Alonso, 2021)

Obligaciones de las empresas

Según Checa, (2019) La regulación de protección de datos se aplica tanto a empresas privadas y del sector público, lo que trae nuevos desafíos relacionados con la privacidad y su proceso de cumplimiento, lo que requiere que una organización tome acciones relacionadas con la gestión de riesgos de protección de datos, las mismas que hay que considerar desde tres aristas:

Figura 1

Aristas por cumplir en la LOPD

Nota: Elaboración propia, en el gráfico se presenta las aristas principales que se basa en regulación de DP que afecta a las organizaciones.

Principios Básicos de protección de datos

- **Lealtad y transparencia:** Para el titular de los datos personales debe quedar claro la utilización de estos datos y es transparente ya toda información debe ser transparente y precisa, manejando un lenguaje sencillo.
- **Exactitud:** La información deben ser exacta, en caso de errores deben ser actualizados y adoptar medidas razonables.

- **Permanencia y Minimización:** Los datos recogidos deben ser limitados, orientados a cumplir con la finalidad del tratamiento y deben mantenerse únicamente en el periodo establecido hasta que se cumpla su objetivo.
- **Integridad y confidencialidad:** Precautela la integridad y seguridad de los datos, de manera que se conserven los mismos, no debe existir modificación o alteración, Todas los involucrados en el procesamiento de datos personales deben respetar el principio de confidencialidad.

Estructura de la LOPD

A continuación, se detalla de manera resumida la estructura de la ley orgánica de datos personales.

CAPÍTULO I: Ámbito de Aplicación Integral

En este capítulo consta de 9 artículos que se detallan el objetivo principal de la ley, existe información de cómo se encuentra establecido los datos personales, los responsables, los términos y definiciones que están establecido a lo largo de la ley.

CAPÍTULO II: Principios

Está constituido por un solo artículo, que contempla 13 principios, estos principios están enfocados en la seguridad y en el tratamiento de datos que se debe entregar a los mismos, en este capítulo se encuentran las mejores prácticas en materia de seguridad de la información.

CAPÍTULO III: Derechos

Existen 14 artículos que se encuentran detallados los derechos, se especifican la relación entre las ciudades y el responsable del procedimiento de los datos personales, mediante este capítulo es posible indicar la interacción y las solicitudes que debe realizar el titular al responsable de los datos.

CAPÍTULO IV: Categorías Especiales De Datos

La ley busca proteger los datos personales y el uso que le da a cada uno de ellos. Este capítulo detalla 8 artículos que tienen como característica principal proteger los datos sensibles que deben ser precautelados con cuidados adicionales.

CAPÍTULO V: Transferencia o comunicación y acceso a datos personales por terceros

El presente capítulo establece que existe la capacidad de identificar si los datos personales han sido entregados a un tercero y los datos personales pueden transferencia o comunicar a terceros nacionales o extranjeros, tales como afiliados o empresas relacionadas o proveedores de servicio, siempre y cuando dispongan de la respectiva autorización por parte del titular de los datos

CAPÍTULO VI: Seguridad de datos personales

En este capítulo es posible identificar si la gestión de cada empresa u organización se encuentra en riesgo, consta de 10 artículos que detalla información sobre el análisis, riesgos y amenazas que se debe detectar sobre el tratamiento de los DP, en este ámbito se debe entender como la protección que deben manejar las distintas empresas para cumplir con la ley.

CAPÍTULO VII: Del responsable y el delegado de protección de datos personales

En este capítulo se detalla información sobre las responsabilidades de los encargados de los datos personales, consta de 5 artículos, en cada uno de estos se informan los roles que debe tener cada uno de los responsables.

Según Eras, (2021) El rol del Delegado de Protección de Datos Personales, es un rol que necesariamente debe estar establecido en las instituciones de la Administración Pública conforme a lo indicado en la siguiente cita del Art. 48, numeral 1 «Cuando el tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República», esto también es aplicable a instituciones privadas, siempre que exista la necesidad de control es este tipo de datos personales y por supuesto un gran volumen de transacciones con esta data , por lo que se debe considerar tener o externalizar este rol en sus organizaciones.

CAPÍTULO VIII: De la responsabilidad proactiva

En la responsabilidad proactiva se puede entender que hay referencia de las distintas normas ISO del grupo 27701 para que se genere confianza en el procesamiento de los datos personales, implementando mejoras continuas en la normativa.

En estos 3 artículos se espera una exactitud consciente, pulcra y efectiva por parte de la organización.

CAPÍTULO IX: Transferencia o comunicación internacional de datos personales

Capítulo compuesto por 6 artículos, en este capítulo se trata el manejo adecuado de datos entre empresas nacionales e internaciones, en esto artículos definen los lineamientos para el traslado internacional.

CAPÍTULO X: de los requerimientos directos y de la gestión del procedimiento administrativo

El capítulo X permite dar a conocer que el titular puede presentar en cualquier momento requerimientos, peticiones, quejas o reclamos directamente al encargado del tratamiento de datos. La autoridad de protección de datos puede comenzar a procesar la solicitud a petición del propietario.

CAPÍTULO XI: Medidas correctivas, infracciones y régimen sancionatorio

El presente capítulo se puede identificar las multas o sanciones que se establecerán a las organizaciones al no cumplir con lo establecido.

CAPÍTULO XII: Autoridad de protección de datos personales

Consiste de 3 artículos que detallan cuál será la autoridad en proteger la información de datos personales, en Ecuador la superintendencia tiene la obligación de dar vida a la ley.

La LOPD está basada en el RGDP que fue aprobado por el parlamento europeo,

Importancia del consentimiento y finalidad

A lo largo de la vida, toda persona entrega su información personal sin las medidas necesarias, ya que confían que le van a dar un buen uso de estas, según (Felipe, 2021) la principal problemática en la mayoría de los casos se da debido a que el titular no reconoce ni autoriza ningún proceso de gestión con sus datos personales. Y en el caso de que, si acepte este proceso, siempre se genera una duda sobre si los datos obtenidos son o cumplen dicho objetivo.

En LOPD establece que la característica principal para el titular acepte el uso de sus datos es que debe ser libre, especificó, informado, incuestionable y las condiciones principales debe ser demostración, distinción, revocación y libertado con esto debe ser la comunicación libre por parte del interesado para que se pueda dar a sus datos personales. Al solicitar el consentimiento las empresas deben ser claras en sus solicitudes, para que el responsable pueda entender cuál va a ser la utilidad que se le va a dar.

Para evitar sanciones en la ley en base al consentimiento es importante que se pueda verificar cada uno de los artículos establecidos en la ley.

Importancia de la seguridad de la información

Según Sampedro, et al, (2019) La seguridad de la información es un conjunto de medidas proactivas y reactivas que las organizaciones deben producir e implementar: políticas, estándares, procedimientos, análisis de riesgos, planes de contingencia, entre otras medidas encaminadas a mantener y asegurar la confidencialidad, integridad y disponibilidad de la información.

Con esto se puede identificar que la seguridad de la información estaba basada en proteger los datos que pasan a ser, los activos de la empresa, ya que se puede evaluar los riesgos y así poder evitar los mismos.

Todas las empresas, organizaciones e individuos se han visto involucrados en interactuar mediante dispositivos inteligentes ya que esto agilizará el proceso de transferencias y comunicación en distintas índoles y estos movimientos mediante el aplicativo móvil se realizan a diario, es por esto que el robo de información es una preocupación del día a día de las empresas, por ende, la seguridad de la información tiene un papel importante en la actualidad.

Según Morales, et al, (2019) Actualmente vivimos en la era de los cambios digitales, cuando las empresas y especialmente la información se han trasladado a medios digitales, lo que significa un desafío aún mayor para las organizaciones para proteger sus datos. Según Fortinet, cada minuto se infiltran 54500 empresas y cada 60 segundos se neutralizan más de 140000 programas maliciosos en todo el mundo. Los elementos que contemplan un buen proceso de resguardo de los datos críticos son:

- Integridad
- Disponibilidad
- Confidencial

La data de cada empresa es vital ya que pueden llegar a guardar información desde hace muchos años atrás y esto nos puede ayudar a identificar movimientos de las empresas, mejorar procesos actuales entre otras cosas más.

Pérdida de Información

La pérdida de información puede ser tan perjudicial para cada una de las empresas que pueden llegar hasta llegar a ser pérdidas económicas. Las causas más comunes de pérdida de información son errores humanos, fallos eléctricos, virus, secuestro de archivos.

Todas las empresas a nivel mundial siempre están alertas ante los ciberataques, según Ironhack, (2020), Según un estudio realizado el primer país en sufrir más ataques por ciberdelincuentes es España después se encuentran Estados Unidos y Alemania. Algo que se ratifica de acuerdo con las evaluaciones de riesgo realizadas por expertos probados en todo el mundo. Por ejemplo, según el informe DsiN-Praxisreport publicado en octubre del año 2020 por lo menos la mitad de las empresas (46%) reportaron ataques cibernéticos en ese año.

Todos los países a nivel mundial se encuentran en alerta por los ciberataques, ya que la informalidad que existe en el ámbito de la información puede hacer que las organizaciones puedan llegar a perder información, esta informalidad se puede visualizar en ecuador ya que la seguridad a nivel de información no estaba siendo tomada en serio hasta que los ataques fueron pérdidas de considerables sumas, aun a ecuador le hace falta actualizaciones a nivel general.

Según Contero, (2019), las organizaciones que deseen implementar un proceso que regule todo el ámbito relacionado a seguridad de la información basada en normativas internacionales deben trabajar en una política de seguridad de la información, para este proceso se puede desarrollar de acuerdo a la norma ISO 27000 y su familia de normas; El tratamiento de las buenas prácticas relacionadas con la seguridad de la información puede basarse en la norma ISO/IEC 27002.

Es importante resaltar que ningún país se encuentra exentó de los ciberataques ya que cada país tiene información sensible como lo es el ámbito económico, los ciberdelincuentes siempre están a la par de la tecnología y están buscando la manera de ingresar a la red de las empresas para poder robar o secuestrar la información que es el ataque común actualmente. Se ha podido evidenciar que la forma más fácil de llegar a la información es por parte del ser humano ya que el desconocimiento general sobre los distintos peligros que existen.

Conductas que pueden generar Sanciones

Las sanciones se pueden dividir en graves y leves, para el caso de sanciones graves la ley nos indica que la multa será entre 10 a 20 salarios básicos unificados, siempre que exista un responsable o dueño del proceso del manejo de datos personales, generando una sanción será entre 0.7% al 1% calculado sobre el volumen de su negocio.

2.2. Descripción de la Propuesta

De acuerdo al análisis realizado, los datos personales coexisten en un ambiente físico o digital, debido a la rápida evolución tecnológica a la que se afrontan la mayoría de las empresas, se hace evidente que el conservar los datos es más fácil, productivo y económico, si se los mantiene en un ambiente digital, es por esto que la ley exige que las organizaciones garanticen la seguridad de esta información antes de adquirirlos , esto a su vez está orientado a la ciberseguridad, por lo que mediante un cuadro comparativo podemos verificar las ventajas de la ciberseguridad y la ley.

Tabla 1:

Ventajas de LOPD y Ciberseguridad

Ventajas	
LOPD	**Ciberseguridad**
La ventaja principal es tener la tranquilidad de que la información confidencial se encuentra resguardada.	Posibilidad de hacer frente a la ciber amenazas preventivas y correctivas y evitar filtraciones y accesos no autorizados, así como repercusiones legales, sanciones. IEC/ISO 2001
Transmitir tranquilidad a todos los clientes, sobre el uso y manejo adecuado de sus datos personales.	La detección de amenazas y vulnerabilidades es fundamental para mantener segura y protegida la información privada de las empresas. IEC/ISO 2001

Nota: Elaboración propia

Técnicas de medidas de Seguridad

Según ISO/IEC 27001, se detalla distintas acciones que ayudan a proteger el ámbito digital.

- Limitar el acceso a la base donde se encuentra la información, únicamente pueden ingresar usuarios autorizados.
- Verificar el proceso inicial de seguridad para la adquisición, manejo, gestión y mantenimiento tanto de componentes físicos como lógicos
- Proteger los recursos, tecnológicos o cualquier información física o electrónica que pueden salir de la organización.
- Política de seguridad
- Administración de incidentes
- Gestión de las actualizaciones para solventar las vulnerabilidades.
- Cifrado de archivos, discos duros y memorias USB.

Tabla comparativa en la cual puede identificar como puntos principales de las bases jurídicas (Tabla2) y lo que se encuentra actualmente en la empresa.

Tabla 2

Bases Jurídicas para el tratamiento de datos personales

Disposiciones	**Actividades**	**Resultados Deseados**
Consentimiento	• Consentimiento verificable del usuario	Los distintos términos y políticas de privacidad deben presentarse de forma legible.
	• Registro de Consentimiento	Mantener un registro claro del consentimiento otorgado.
Derecho a ser informado	• Informar a los usuarios sobre el manejo de sus datos	Aviso o política de privacidad**.**
Derecho de acceso	• Acceso a sus datos personales y conocer cómo lo tratan	Proporcionar a la persona solicitante una copia gratuita de sus datos personales.

Derecho de rectificación	• Si sus datos personales son inexactos o están incompletos, puede solicitar su rectificación.	solicitud de rectificación
El derecho de oposición	• Pueden oponerse a ciertas actividades de tratamiento de sus datos personales, realizadas por el responsable.	Solicitud del derecho de oposición
El derecho a la portabilidad	• Obtener sus datos personales con el fin de transferirlos	Solicitud de portabilidad de datos
El derecho de eliminación	• Solicitar que se eliminen su información personal y a que se cese toda difusión de estos, cuando los usuarios hayan retirado su consentimiento	Solicitud de eliminación
Derecho a la educación digital	• tiene derecho al acceso y disponibilidad, de conocimiento.	Generar guía para que el titular conozca sus derechos.

Nota: Elaboración Propia

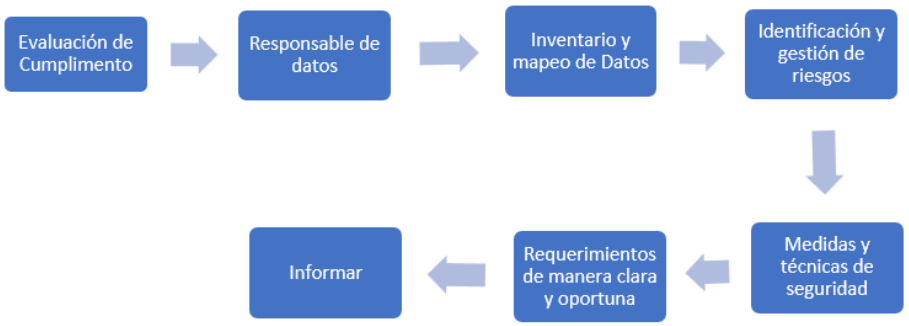
Registro de actividades sobre el tratamiento

En base a la LOPD, toda organización está obligada a documentar las actividades de tratamiento que se realizan bajo su responsabilidad a la información personal, te explicamos cuál es la clave para la correcta realización de estas actividades. (Cabello, 2019)

a) Estructura General

Figura 2

Estructura de Implementación



Nota: Elaboración Propia

b) Explicación del Aporte

En la Figura 2. se observa cómo implementar un sistema de protección de datos en las distintas empresas, la serie de pasos presentada permite de forma ordenada identificar cuáles son los datos personales y llegar a cumplir con lo requerido en la ley.

Tabla 3

Estructura de Implementación

Estructura	Detalle
Evaluación de Cumplimento	Analizar la situación actual con mediante un análisis GAP a las distintas áreas interesadas.
Responsable de datos	Se debe designar un responsable de tratamiento de datos, para que el proceso de implementación vaya en conjunto y sea el responsable de cuidar lo que se haya recolectado.
Inventario y mapeo de Datos	Identificación de la fuente de datos y clasificar el tipo de datos que mantiene la

	empresa, para poder identificar que datos son confidenciales o privados.
Identificación y gestión de riesgos	Realizar un análisis minucioso de la estructura física y software que mantiene la organización, para poder identificar las amenazas que pueden presentarse.
Medidas y técnicas de seguridad	Con base en el análisis de riesgo, se deben implementar procesos de seguridad que garanticen la confidencialidad, integridad y disponibilidad.
Requerimientos de manera clara y oportuna	Se debe realizar un proceso que permita de manera clara receptar las solicitudes realizadas por el titular y entregar respuestas efectivas.
Informar	El responsable de tratamiento de datos debe informar a los titulares o interesados, el tratamiento, que ocurre con sus datos.

Nota: Elaboración Propia

c) Técnicas

Para el desarrollo de esta investigación se consideró de vital importancia el generar un acercamiento con responsables en la toma de decisiones de empresas en el departamento de seguridad, de esta forma y mediante los resultados obtenidos poder garantizar las mejores prácticas para conseguir los resultados deseados.

2.3. Validación de la propuesta

Para validar la propuesta a continuación, en la Tabla 4, se detalla los procesos aplicados en la empresa respecto a la ley.

Tabla 4

Análisis de la LOPD y la organización

LOPD	Que dispone actualmente	Análisis	Seguridades a Implementarse	Porcentaje de Cumplimento
Registro y Comunicación Términos y políticas de privacidad claras y legibles	• Notificación en página web • correos electrónicos • Contrato de confidencialidad con los usuarios	En enero del año 2023 la empresa contrata consultoría externa para regular información de pie de email y notificaciones a nuestros clientes que, por cumplimiento de normativas de la ley de protección de datos, se incluyen en firmas de correo electrónico una sección de Aviso de confidencialidad que hace referencia al capítulo 3 de la Ley de protección de datos personales.	Debe existir un apartado que permita aprobar la política de privacidad, donde se detalle cuál es la finalidad, tratamiento que se entregarán a los datos. Esta aprobación se debe incluir en el aplicativo móvil y en la web al ingresar por primera vez al sistema	50%
Registro del consentimiento otorgado	No dispone de mecanismos de autorización	La empresa debe generar una campaña con todos sus clientes con el fin de que entreguen un consentimiento en el que se detalle la finalidad y el tratamiento que se darán a estos datos.		0%
Solicitud de datos personales				0%

	No existe un detalle o un proceso interno establecido para la entrega de los datos personales a un titular.	Es importante que se mantenga un registro y responsable de la solicitud que se realizan para la entrega de los datos personales al titular	Una vez ingresada la solicitud, el sistema permite enviar los datos de forma automática	
solicitud de rectificación/actualización	Actualmente si un titular de datos personales requiere que se realice el cambio o rectificación de sus DP, únicamente se comunica con el gerente o la parte administrativa de la empresa y se realiza el cambio.	Se debe realizar y notificar una solicitud formal que permita identificar al titular de los datos y la información que se debe actualizar. se debe realizar un proceso establecido en el cual intervenga el responsable de dato en la organización	Se debe tener un log que permite visualizar que fecha, responsable, y el dato que se actualizo o modifico	0%
Solicitud del derecho de oposición	No dispone de mecanismos de autorización	Al no tener un registro y una política clara y aceptada, los titulares de los datos no conocen el proceso a oponerse sobre el tratamiento que estén realizando a sus datos. En este punto se debe realizar un proceso que incluya una solicitud o un formulario que permita informar al responsable de datos.	Se debe implementar en el software que permita la visualización y anulación del consentimiento otorgado que entregó el titular	0%
Solicitud de portabilidad de datos	No dispone de mecanismos de autorización		El envío de información debe ser de manera automatizada resguardando que la	0%

		El ciudadano puede exigir a las empresas que estén tratando sus datos, que se los devuelvan o que los pasen a otra empresa.	información no pierda su integridad.	
		Al ser una empresa que presta servicios de un software a distribuidores de consumo masivo, la eliminación de un dato personal se torna complejo, ya que sería importante eliminar el historial del usuario antes de realizar el proceso de eliminación.		
Solicitud de eliminación	No dispone de mecanismos de autorización	Es importante implementar un procedimiento que permita ingresar la solicitud y realizar la eliminación de los datos.	Para este punto los sistemas deben permite realizar un borrador de la información, de forma automatizada	0%

Nota: Elaboración Propia

El resultado evidentemente muestra que a pesar de que la empresa tiene implementado la política de privacidad el nivel de cumplimiento tiene un porcentaje del 0%, esto quiere decir que se requiere implementar estos procesos en la organización, al momento el no poseer estos procesos en su totalidad y apenas cubrir parcialmente un punto al 50%, deja muestras claras de que no está preparada para afrontar el proceso, existen puntos críticos que se deben atender con urgencia por el poco tiempo que queda ya para la adaptación de la ley.

Este proceso de adaptación generará cambios fuertes en reglamentos internos de la empresa para poder llegar a cubrir lo requerido por la ley y garantizar el correcto cumplimiento hacia los clientes.

De acuerdo con el análisis realizado en la tabla 3, se describe las distintas sugerencias que se pueden aplicar en la organización.

Tabla 5:

Soluciones de acuerdo a las bases jurídicas de la LOPD

Motivos y Sugerencias	
Los términos y políticas de privacidad deben presentarse de forma legible.	Comunicar y detallar de manera clara las políticas de privacidad establecida en la empresa. La política debe contener información de la obtención y la finalidad.
Mantener un registro claro del consentimiento otorgado.	Conservar copias de seguridad en nube y bajo control de personal autorizado
Proporcionar a la persona solicitante una copia gratuita de sus datos personales.	Se debe proporcionar copia de la información personal previa solicitud.
solicitud de rectificación	La solicitud requerida debe estar de manera clara quien es el titular de los datos, la respuesta debe ser de manera clara y oportuna.
Solicitud del derecho de oposición	La comunicación con los interesados debe ser en todos los casos concisa, transparente y disponible en un lenguaje claro y sencillo. Si la solicitud se presenta por vía electrónica, la respuesta también deberá darse por este medio, salvo que el interesado haya indicado lo contrario.
Solicitud de portabilidad de datos	En la solicitud debe encontrarse de manera clara la información del titular de los datos y le medio de envió.
Solicitud de eliminación	Eliminar o encriptar la información en base a la solicitud.

Nota: Elaboración propia

Al implementar controles de seguridad y adaptar una cultura de protección de datos, tendrá un impacto social positivo para el cumplimento de la normativa (Calisaya & Tarrillo, 2018).

Responsable del tratamiento de datos

La empresa Mobilvendor tiene un departamento de TI la cual regula y administra mediante procesos de ITIL V3 sus procesos informáticos, también se cuenta con niveles de aprobación a nivel de gerencia general y del departamento jurídico en donde se validan temas de protección de datos.

Análisis de riesgos

De acuerdo con estos resultados se logra identificar de manera general que existen riesgos potencialmente altos debido a la criticidad del servicio que presta la empresa, pero no se encuentra establecida un análisis de riesgos y una matriz de riesgos.

Hay que tener en cuenta que se debe incluir también un apartado para el cifrado de información en caso de que exista pérdida del equipo celular de un vendedor y pueda comprometer información sobre datos personales de los clientes, esto llevaría modificar también el uso de la aplicación móvil hacia estándares.

Para el análisis de riesgos se debe basar en los siguientes puntos:

- Identificar Amenazas y riesgos
- Evaluar los riesgos
- Tratar los riesgos

Este punto es importante ya que la ley está orientada a la protección de información.

- **Eliminación**

La empresa debe implementar un proceso que permita eliminar los identificadores de datos personales, esto se puede realizar, esto es una herramienta que permite mitigar los riesgos y así evitar la divulgación de datos personales.

- **Garantías**

La empresa garantiza, confidencialidad, integridad, disponibilidad, resiliencia, en la protección de DP, ya que toda información con la que transacción se almacena en servidores de Amazon web service y este proveedor de servicios cuenta con herramientas de seguridad, es compatible con 98 estándares de seguridad y varias certificaciones, con esto la empresa asegura estándares de seguridad.

Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 6:

Matriz de Articulación de la propuesta

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Ley Orgánica de Datos Personales Ecuador	Ley que permite garantizar el derecho a la protección de datos personales.	La metodología de investigación fue bibliográfica que permitió obtener información de la Ley.	Fuente Bibliográfica	Analizar la estructura y características de la LOPD.	
Reglamento General de Protección de Datos (RGPD)	El Reglamento General de Protección de Datos (RGPD) es el nuevo marco jurídico de la Unión Europea que rige la recopilación y el tratamiento de los datos personales	La metodología de investigación bibliográfica	Fuente Bibliográfica	Analizar los distintos derechos y estructura de la RGDP	

CONCLUSIONES

Se había indicado que los datos personales son los activos más significativos para las distintas organizaciones, con el avance de la tecnología se puede identificar que la información llega a tener vulnerabilidades y con esto nace la necesidad de contar con una adecuada protección de datos que genere igualdad entre los derechos y el desarrollo económico.

Los sistemas deben cumplir con el objetivo de proteger la información de datos personales, debe ser prioritario que los sistemas que se manejan actualmente garanticen el derecho la protección y acceso de la información de manera esto genera confianza y seguridad en el mundo digital.

Considerando que la LOPD trabaja en conjunto con diferentes Marcos de trabajo tecnológicos, es entendible que en el proceso de seguridad de la información participan ordenadamente expertos en la rama de sistemas y jurídicos principalmente, así como también otras partes de la organización.

Los estándares europeos de protección de datos son pioneros en la protección de datos personales, centrándose en la seguridad de la información, en años anteriores se ha podido evidencia que las distintas empresas se estaban orientado a la protección de su información y más no de los clientes, es por esto que desde el LOPD se realizó el ajuste y con esto proteger los datos a nivel de general de todos los ciudadanos y no únicamente de las empresas.

De acuerdo al análisis de brechas realizado se puede identificar que una de las ventajas que tiene la empresa es que toda la información es almacenada en la nube de Amazon web service, este servicio cuenta con protección de datos cifrado y administrado por claves, monitorea constantemente amenazas que protegen continuamente las cargas de trabajo.

Los datos personales tienen un valor económico y social, al cumplir con la ley establecida de protección de datos personales generan seguridad a los clientes.

De acuerdo al objetivo número nueve de innovación e infraestructura se puede evidenciar que la aplicación de esta ley en el país deben generar cambios significativos en base a la seguridad de la información y esto con lleva cambios en infraestructura para mitigar e riesgo.

RECOMENDACIONES

No existe un detalle de parte de los responsables sobre el uso y tratamiento que se debe entregar a los datos personales, se debe asignar un procedimiento interno donde el departamento de TI basado en las mejores prácticas de aplicación de la ley asuma la responsabilidad del manejo de datos.

Al realizar teletrabajo se recomienda realizar una política de privacidad para la movilidad, donde se defina conexión de manera remota, se debe definir responsabilidades y obligaciones a cada empleado. Todos los empleados deben estar conscientes de las amenazas y las consecuencias al ser atacados.

Se recomienda implementar procesos de ISO 27001 sobre seguridad de la información ya que son un conjunto de normas internacionales dirigidas a optimizar la gestión de empresas en diferente ámbito, esta norma se basa en la mejora continua e integra gestión de riesgos de seguridad sobre la información y privacidad, esta norma facilita el cumplimiento con la Ley organiza de datos personales.

Se recomienda restringir acceso a la información, los permisos deben configurarse de acuerdo con el rol de cada persona, es importante aplicar restricciones de ingreso a seguridad privada, se debe guardar información de los cambios, modificaciones que realiza cada empleado sobre la información registrada en el sistema.

BIBLIOGRAFÍA

Alejandra Benavides Sepúlveda, C. B. (2018). *Scientia et Technica Año XXI.* Obtenido de Modelo sistema de gestión de seguridad de la: https://www.redalyc.org/journal/849/84956661012/84956661012.pdf

Alonso, C. (2021). *Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador*. Obtenido de https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/

Arellano, C. (2020). El derecho de protección de datos personales. *Biolex*, 163-174. doi:https://doi.org/10.36796/biolex.v0i23.194

Arteaga, G. (10 de 2020). *Investigación bibliográfica – Cómo llevar a cabo una*. Obtenido de https://www.testsiteforme.com/investigacion-bibliografica/

Brunet, L. N. (2015). Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. *Revista de la Facultad de Derecho*. Obtenido de http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301-06652015000200009&lng=es&tlng=es

Cabello, C. (2019). *RGPD: claves para llevar correctamente el registro de actividades de tratamiento de datos*. Obtenido de https://www.sage.com/es-es/blog/rgpd-claves-para-llevar-correctamente-el-registro-de-actividades-de-tratamiento-de-datos/

Cabezas, F. (2018). *Creación de un sistema de comercialización.* UNIVERSIDAD TÉCNICA DE AMBATO, Ambato. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/28182/1/707%20MKT%20sp.pdf

Calisaya, C., & Tarrillo, M. (2018). *Implementación de controles de seguridad para la protección de.* lima. Obtenido de file:///C:/Users/USER/Downloads/Cristhian_Tesis_Titulo_2018%20(con%20enlace).pdf

Checa, F. (2019). *IT ahora*. Obtenido de https://itahora.com/2019/09/30/los-desafios-empresariales-frente-a-la-nueva-regulacion-de-proteccion-de-datos/

Coba, G. (29 de 04 de 2021). *Primicias*. Obtenido de https://www.primicias.ec/noticias/economia/compras-consumo-masivo-crecimiento-ecuador/

Colombato, I. &. (2021). Tensiones entre el derecho al acceso a la información y la protección de datos personales en la vacunación contra el COVID-19 en Argentina. *Millcayac, VIII(15)*, 27-54. doi: https://www.redalyc.org/articulo.oa?id=525869069003

Contero, W. (2019). DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN. *Tesis de Maestria.* Universidad Internacion Sek, Quito. Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Datos., A. E. (2019). *Red Iberoamericana de Protección de Datos*. Obtenido de https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd

ECUCERT. (2021). *ARCOTEL - EcuCERT*. Obtenido de https://www.ecucert.gob.ec/estadisticas/

EMIS. (2021). *EMIS*. Obtenido de https://www.emis.com/php/company-profile/EC/Mobilvendor_Software_Company_CiaLtda_es_4905741.html

Enríquez Álvarez, Luis. "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. 27 (I Semestre, 2017): 43-61. https://repositorio.uasb.edu.ec/handle/10644/5945

Enriquez, O. A. (2018). Protection of Personal Data in Companies Established in Mexico. *Revista IUS*.

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

Felipe, R. (2021). *Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador.* USFQ Law, Quito. doi:10.18272/ulr.v8i1.2184

Gobierno de España. (05 de 2016, 27 de abril). *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.* Agencia Estatal Boletin oficial del Estado. Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Gregorio, C., & Ornelas, L. (2011). *PROTECCIÓN DE DATOS PERSONALES.* Mexico. Obtenido de https://libros.metabiblioteca.org/bitstream/001/307/9/978-968-5954-59-4.pdf

Guerrero, P. (2020). *Los derechos digitales en Europa tras el Reglamento de Protección de Datos Personales: Un antes y un después del derecho al olvido.* España. doi:ISSN 0718-5200

Guzman, J. (2019). Unidades de Apoyo para el Aprendizaje. CUAED/Facultad de Contaduría y Administración. *Técnicas de Investigación de Campo.* Obtenido de https://uapa.cuaieed.unam.mx/sites/default/files/minisite/static/0fecd888-6a3f-4b31-b704-a2d94e3eed72/U000308176506/index.html

Huerta, P. (2017). La génesis del derecho fundamental a la protección de datos. *(tesis Doctoral).* Universidad Complutense Madris, Madrid. Obtenido de E-Prints Complutenserepsitoria institucional de la UMC

Ironhack. (10 de 2020). *Análisis: los países más amenazados por los ciberdelincuentes y los piratas informáticos en 2020*. Obtenido de https://www.ironhack.com/es/noticias/analisis-los-paises-mas-amenazados-por-los-ciberdelincuentes-y-los-pira.

ISO/IEC 27001 and related standards. (2023b). ISO. https://www.iso.org/isoiec-27001-information-security.html

kasperky. (2021). *CIBERAMENAZA MAPA EN TIEMPO REAL*. Obtenido de https://cybermap.kaspersky.com/es

Legal Alert. (2021). *Building a better working world*. Obtenido de

file:///C:/Users/USER/Downloads/ey-legal-alert-resumen-ley-proteccion-datos-personales.pdf

Meltezer, J. P. (08 de 2018). *Banco Internacional de desarrollo.* Obtenido de https://publications.iadb.org/publications/english/document/A-Digital-Trade-Policy-for-Latin-America-and-the-Caribbean.pdf

Mendoza, A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista IUS*. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). Obtenido de https://www.telecomunicaciones.gob.ec/el-ministerio/

Morales, F., Toapanta, S., & Toasa, R. (2019). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información.* Universidad Tecnológica

Israel, Quito.https://www.researchgate.net/profile/Renato-Mauricio-ToasaG/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Implementacion-de-un-sistema-de-seguridad

Morales, N. (2015). Investigación exploratoria: tipos, metodología y ejemplos. Recuperado de https://www. lifeder. com/investigacion-exploratoria

Ocampo, D. S. (2019). Obtenido de https://investigaliacr.com/investigacion/investigacion-bibliografica/

OMC. (2018). *Informe sobre el comercio mundial 2018.* Obtenido de https://www.wto.org/spanish/res_s/publications_s/world_trade_report18_s.pdf

Porcelli, A. (2019). *LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ENTORNO DIGITAL.* Rio de Janeiro. doi:10.12957/rqi.2019.40175

Roldán Carrilo, F.N. «Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador». USFQ Law Review, Vol 8, no 1, mayo de 2021, pp. 175 - 202, doi: 10.18272/ulr.v8i1.2184

RODRÍGUEZ, ORTIZ, QUIROZ, PARRALES. (2020). El e-commerce y las Mipymes en tiempos de Covid-19. doi:10.48082/espacios-a20v41n42p09

Sampedro, C., Machuca, S., Palma, D., & Carrera, F. (2019). *PERCEPCIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN SANTO DOMINGO.* REVISTA INVESTIGACIÓN OPERACIONAL, Ambato.

Santa Gadea, K., Gadea, W., & Vera, S. (2017). Rompiendo Barreras en la Investigación. En K. D. Quiñonez. Machala: Editorial UTMACH, 2018. doi:978-9942-24-087-3

Sosa Umbo, O. A. (2022). Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los beneficiarios del Bono Universal en el Perú.

Tamayo, M. (2003). *El proceso de la investigación científica. (4ª ed) Limusa*. https://www.gob.mx/cms/uploads/attachment/file/227860/El_proceso__de_la_investigaci_n_cient_fica_Mario_Tamayo.pdf