Pontificia Universidad Católica del Ecuador
Seréis mis testigos
ESMERALDAS

ESCUELA DE DERECHO

Tema:

PROTECCIÓN DE DATOS PERSONALES: LA RESPONSABILIDAD LEGAL DE EMPRESAS EN CASOS DE VIOLACIONES DE SEGURIDAD CIBERNÉTICA EN EL MARCO LEGAL ECUATORIANO.

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

Línea de investigación:

ESTADO, DERECHO Y SOCIEDAD

Autor:

Bruno Enrique Vera Bergamaschi

Director:

Abg. Santiago Javier Paliz Ibarra Mg.

Esmeraldas - Ecuador

Marzo 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **BRUNO ENRIQUE VERA BERGAMASCHI**, con cédula de ciudadanía **0803228170**, autor del trabajo de graduación titulado: “Protección De Datos Personales: La Responsabilidad Legal De Empresas En Casos De Violaciones De Seguridad Cibernética En El Marco Legal Ecuatoriano.”, previa a la obtención del título profesional de **ABOGADO**, en la escuela de **DERECHO**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación 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. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Esmeraldas, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Esmeraldas, marzo 2025

Bruno Enrique Vera Bergamaschi

CC. 0803228170

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema: Protección De Datos Personales: La responsabilidad legal de empresas en casos de violaciones de seguridad cibernética en el marco legal ecuatoriano.

Línea de investigación:

ESTADO, DERECHO Y SOCIEDAD

Autor:

Bruno Enrique Vera Bergamaschi

Santiago Javier Paliz Ibarra, Ab. Mg. f._____

ASESOR

Manaces Esaud Gaspar Santos, Ab. Mg. f._____

CALIFICADOR

Laura Zulima Duque Jironza, Ab. Mg. f._____

CALIFICADOR

Andrés Sebastián Heredia Alvear, Ab. Mg. f._____

COORDINADOR ESCUELA DE DERECHO

Dra. Mariana de Jesús Verduga Álvarez f._____

SECRETARIA GENERAL PUCESE

Esmeraldas – Ecuador

Marzo 2025

DEDICATORIA

Dedico este trabajo a mi familia, cuyo esfuerzo y sacrificio me han permitido hacer realidad este sueño. A mi padre, quien con su ejemplo me enseñó el verdadero significado de los valores, la justicia y la perseverancia en los momentos difíciles. A mi hermano, compañero de vida, que me apoyó en mis altos y bajos, y cuya existencia fue mi mayor inspiración para seguir adelante y convertirme en un modelo digno para él. Y a mi abuela, cuyo amor incondicional y cálido afecto maternal fueron un refugio y una guía en mi camino, dejando en mí enseñanzas que han sido un pilar fundamental en mi desarrollo como abogado. A ustedes, que han sido mi fuerza y mi razón, les debo este logro. Gracias por creer en mí.

AGRADECIMIENTO

Agradezco de corazón a mis profesores, quienes con paciencia, dedicación y entrega me guiaron en este camino, enseñándome que el derecho no es solo una profesión, sino un compromiso de vida con la justicia. En especial, al profesor Andrés Heredia, cuya pasión y conocimiento fueron mi fuente de inspiración desde el primer día de clases con él. A mis amigos y compañeros, por cada risa, aprendizaje y momento compartido, que hicieron más llevadero este viaje y me dieron fuerzas en los días difíciles. A mi familia, por su amor incondicional, su apoyo constante y su fe en mí, incluso en los momentos de duda. Y a todas aquellas personas que, de una u otra manera, contribuyeron a mi formación como abogado. A todos, gracias.

RESUMEN EJECUTIVO

El presente trabajo analiza la protección de datos personales en Ecuador, con especial énfasis en la responsabilidad legal de las empresas ante violaciones de seguridad cibernética. Se examina la autodeterminación informativa como derecho fundamental que permite a los individuos controlar el uso de su información y se estudia la Ley Orgánica de Protección de Datos Personales, que establece principios como la transparencia, confidencialidad y seguridad en el tratamiento de datos. Asimismo, se analiza la responsabilidad de las empresas, destacando la necesidad de adoptar medidas proactivas de seguridad, como el cifrado y la autenticación de dos factores, para evitar vulneraciones. En caso de incumplimiento, las organizaciones pueden enfrentar responsabilidad civil y sanciones, dependiendo de su diligencia en la protección de la información. Finalmente, se examinan los riesgos derivados de las vulneraciones de seguridad, los efectos de los ciberataques en la confianza digital y la importancia de protocolos efectivos de denuncia y respuesta. Se concluye que una correcta implementación de la normativa y un compromiso real por parte de las empresas pueden reducir significativamente las brechas de seguridad y fortalecer la protección de los derechos de los ciudadanos en el entorno digital.

PALABRAS CLAVES: Protección de datos personales; violaciones de ciberseguridad; responsabilidad legal corporativa; autodeterminación informativa; privacidad de los datos.

ABSTRACT

This paper analyzes the protection of personal data in Ecuador, with a special focus on the legal responsibility of companies in cases of cybersecurity breaches. It examines informational self-determination as a fundamental right that allows individuals to control the use of their information and studies the Organic Law on Personal Data Protection, which establishes principles such as transparency, confidentiality, and security in data processing. Likewise, it analyzes the responsibility of companies, highlighting the need to adopt proactive security measures, such as encryption and two-factor authentication, to prevent breaches. In case of non-compliance, organizations may face civil liability and sanctions, depending on their diligence in protecting information. Finally, the study examines the risks associated with security breaches, the impact of cyberattacks on digital trust, and the importance of effective reporting and response protocols. The research concludes that the proper implementation of regulations and a real commitment from companies can significantly reduce security gaps and strengthen the protection of citizens' rights in the digital environment.

KEY WORDS: Personal data protection; Cybersecurity breaches; Corporate legal responsibility; Informational self-determination; Data privacy.

TABLA DE CONTENIDO

INTRODUCCION 9

CAPITULO I 11

1.1. DATOS PERSONALES 11

1.2. LA AUTODETERMINACIÓN INFORMATIVA 13

1.3. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR 16

1.4. DERECHO A LA EDUCACIÓN DIGITAL 19

1.5. REGISTRO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES 21

1.6. LA PRIVACIDAD EN ECUADOR 22

CAPITULO II 24

2.1. LA RESPONSABILIDAD LEGAL DE LAS EMPRESAS 24

2.1.1. DE LA RESPONSABILIDAD PROACTIVA 26

2.2. PRIVACIDAD Y SEGURIDAD DE DATOS EN EL CONTEXTO DIGITAL 27

2.3. RESPONSABILIDAD CIVIL RESPECTO A DATOS PERSONALES 30

CAPITULO III 33

3.1. VULNERACIÓN A LOS DATOS PERSONALES 33

3.2. PROTOCOLO DE DENUNCIAS Y SOLICITUDES EN PROTECCIÓN DE DATOS PERSONALES 36

3.3. APLICACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES RESPECTO A LA RESPONSABILIDAD LEGAL DE LAS EMPRESAS 39

CONCLUSIONES 41

RECOMENDACIONES 43

REFERENCIAS BIBLIOGRÁFICAS 45

INTRODUCCION

En la era digital, los datos personales han adquirido un valor fundamental, convirtiéndose en un activo clave tanto para individuos como para empresas y gobiernos. La recopilación, almacenamiento y procesamiento de esta información conllevan riesgos significativos, especialmente cuando no se implementan medidas adecuadas de seguridad y transparencia. En este contexto, la protección de datos personales es un derecho fundamental que busca garantizar la privacidad y el control de la información, evitando usos indebidos que puedan vulnerar la dignidad y seguridad de los ciudadanos. Ecuador ha avanzado en esta materia con la promulgación de la Ley Orgánica de Protección de Datos Personales, estableciendo un marco normativo que regula la responsabilidad de quienes gestionan información sensible.

Sin embargo, a pesar de la existencia de regulaciones, muchas empresas aún presentan deficiencias en la implementación de medidas de seguridad, lo que ha llevado a incidentes de violación de datos y a una creciente preocupación sobre la confianza digital. La presente investigación analiza la responsabilidad legal de las empresas en la protección de datos personales, examinando los principios de seguridad, la autodeterminación informativa y los mecanismos de prevención y sanción. Se abordan las vulneraciones a la privacidad, los efectos de los ciberataques y la necesidad de contar con protocolos efectivos de denuncia y respuesta. El objetivo es evidenciar la importancia de una adecuada regulación y compromiso empresarial para fortalecer la seguridad digital y proteger los derechos de los ciudadanos en el entorno tecnológico actual.

Este trabajo es relevante porque, a pesar de la existencia de un marco normativo en Ecuador, las deficiencias en su aplicación han generado

vulneraciones de datos y desconfianza en el entorno digital. Es fundamental analizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales, la responsabilidad legal de las empresas y las medidas de seguridad necesarias para prevenir estos incidentes. Al examinar estos aspectos, la investigación busca contribuir al fortalecimiento de la protección de datos personales y a la creación de un ecosistema digital más seguro y transparente.

CAPITULO I

1.1. DATOS PERSONALES

Según la definición proporcionada por la (Comisión Europea, 2024), los datos personales se definen como “cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal”. Esto incluye no solo incluye información que identifique directamente a una persona como el nombre o su número de cédula, sino también aquella que, combinada con otros datos, permite su identificación indirecta, el criterio debe centrarse en que cualquier dato, directo o indirecto, susceptible de identificar a una persona, que entra en el ámbito de protección del derecho fundamental a la privacidad y a la autodeterminación informativa.

La definición de datos personales proporcionada por la Comisión Europea subraya la amplitud del concepto, abarcando no solo información de identificación directa, como nombres, direcciones o números de identificación, sino también datos aparentemente irrelevantes que, al ser combinados con otros, pueden revelar la identidad de una persona. Este enfoque reconoce que la protección de datos personales no se limita a lo evidente, sino que se extiende a cualquier información que, aunque de forma indirecta, pueda permitir la identificación de un individuo. En este contexto, el derecho fundamental a la privacidad y a la autodeterminación informativa se ve como un mecanismo de protección integral, que garantiza que las personas tengan control sobre sus propios datos, asegurando que su uso no vulnera su dignidad, intimidad o libertad.

Los datos personales, tanto directos como indirectos, son esenciales para la protección de derechos fundamentales, garantizando el control individual sobre la información personal. Es imperativo asegurar un manejo ético de esta información, particularmente en el entorno digital contemporáneo. En este contexto, como señala (Polo, 2021), los datos han cobrado una importancia central en las actividades cotidianas, transformándose en un recurso de gran valor, comparable con el petróleo del siglo XXI, debido a su capacidad para impulsar procesos económicos, sociales y tecnológicos a nivel global.

La creciente importancia de los datos personales en la Sociedad de la Información ha llevado a un aumento en la necesidad de proteger los derechos fundamentales relacionados con la privacidad y la autodeterminación informativa. en la actualidad, los datos se han convertido en un recurso valioso, comparable al petróleo, debido a su capacidad para transformar y dirigir los procesos económicos, sociales y tecnológicos. En este entorno digitalizado, el manejo ético de la información es crucial para evitar abusos que puedan vulnerar la privacidad de los individuos. La gestión responsable de los datos personales no solo es esencial para garantizar el respeto a los derechos de las personas, sino también para fomentar la confianza en el uso de tecnologías emergentes y plataformas digitales.

Ecuador, al igual que muchos otros países, no está exento de los impactos de la Sociedad de la Información, que ha transformado la manera en que las personas interactúan con la tecnología y gestionan sus datos personales. La autodeterminación informativa, que es un derecho fundamental, otorga a cada individuo la capacidad de decidir qué datos compartir, bajo qué condiciones y con qué fines. Este principio refuerza la autonomía de las personas, ya que les

permite tener control sobre su propia información, previniendo posibles abusos, discriminación o vulneración de derechos. Además, al otorgar a los ciudadanos el poder de decidir sobre sus datos, se fomenta una cultura de transparencia y responsabilidad en el manejo de la información.

En este sentido, los datos personales pueden considerarse como extensiones de la personalidad humana, ya que reflejan aspectos íntimos y relevantes de la vida de cada individuo. Por esta razón, su tratamiento debe ser llevado a cabo con el mayor respeto y responsabilidad, garantizando la protección de la dignidad, la privacidad y la integridad de las personas, y evitando cualquier forma de explotación o uso indebido que pueda comprometer sus derechos fundamentales. En un contexto como el actual, donde los datos personales se han convertido en un activo de gran valor, es esencial que existan políticas y regulaciones que aseguren su manejo ético y acorde con los principios de justicia y equidad.

1.2. LA AUTODETERMINACIÓN INFORMATIVA

La autodeterminación informativa según (Adinolfi, 2007) es un derecho fundamental que permite a las personas ejercer control sobre la información personal que les concierne, especialmente en registros públicos y privados. Este derecho está estrechamente relacionado con el derecho a la privacidad y se manifiesta en la capacidad de las personas para decidir sobre la recopilación, almacenamiento y difusión de sus datos personales. Este derecho, en su vínculo con la privacidad, se convierte en una herramienta clave para prevenir la discriminación y el uso indebido de datos que puedan afectar la vida de los individuos en diversos ámbitos, tanto públicos como privados.

La autodeterminación informativa se presenta en como un derecho fundamental que permite a las personas ejercer control sobre su información personal, estableciendo una relación estrecha con el derecho a la privacidad. Si bien la definición es clara, resulta insuficiente en el análisis de los retos que este derecho enfrenta en un entorno digital.

En su investigación sobre tecnologías emergentes, (Hernández et al. 2017) definen Big Data como un conjunto de tecnologías diseñadas para recopilar, almacenar, procesar y analizar grandes volúmenes de datos heterogéneos, cuya generación se produce a una velocidad creciente. La creciente influencia de tecnologías emergentes, como la inteligencia artificial y el big data, pone en jaque la protección de este derecho al incrementar los riesgos de abuso y la dificultad para garantizar su efectivo ejercicio en un contexto tan dinámico.

El vínculo entre la autodeterminación informativa y los derechos de personalidad, así como la libertad de voluntad, es una conexión teórica válida, pero limitada. A pesar de que se reconoce la importancia de estos principios, no se ofrecen ejemplos concretos que permitan al lector comprender las implicaciones prácticas de este derecho, situaciones como el tratamiento de datos en redes sociales, las prácticas invasivas de grandes corporaciones tecnológicas o el uso de información por parte de los gobiernos son cuestiones relevantes que podrían enriquecer el análisis y darle una perspectiva más integral.

Por otro lado, aunque se menciona la autonomía del consentimiento como un elemento central, no se aborda cómo este consentimiento puede verse afectado por prácticas desleales. Por ejemplo, las cláusulas complejas en

políticas de privacidad, los términos y condiciones extensos o la falta de opciones claras para los usuarios dificultan que el consentimiento sea verdaderamente informado y libre. En el contexto de la protección de datos, (Roldan, 2021) define el consentimiento de datos personales como la autorización que una persona brinda de forma libre, informada y expresa para que una entidad recopile, utilice y comparta su información personal. Este consentimiento es esencial en la era digital, donde los datos se consideran un recurso valioso y son objeto de recopilación continua.

Bajo este criterio la autodeterminación informativa es un derecho de vital importancia en la era digital, pero garantizar su efectividad exige un análisis más profundo y crítico de los desafíos estructurales que enfrenta. La implementación de este derecho requiere no solo un marco legal robusto, sino también medidas que promuevan la transparencia, la accesibilidad y la equidad en el tratamiento de los datos personales. Esto demanda una constante actualización jurídica que responda a los avances tecnológicos y a las necesidades sociales.

Tal como lo establece la (Asamblea Nacional del Ecuador, 2021), en la Ley Orgánica de Protección de Datos Personales, se consagra el derecho a la educación digital como una herramienta esencial para garantizar que las personas puedan utilizar las tecnologías de la información y comunicación de manera segura, responsable y respetuosa con los derechos humanos. Este artículo resalta la importancia de fomentar el aprendizaje en temas como la autodeterminación informativa, la privacidad, la protección de datos personales y la ciudadanía digital, convirtiéndose en un pilar fundamental para enfrentar los desafíos de la era digital. Al promover estos conocimientos, se busca empoderar

a los ciudadanos para que tomen decisiones informadas sobre su información personal y su interacción en entornos digitales

Este enfoque resulta particularmente relevante al reconocer que el acceso al conocimiento y la capacitación no solo son un derecho, sino también una necesidad para garantizar el ejercicio pleno de otros derechos relacionados, como la protección de la identidad y la reputación en línea. Al incluir principios como la dignidad humana y los derechos fundamentales, la norma apunta a construir una sociedad digital más equitativa, consciente y preparada para gestionar los riesgos asociados al manejo de información personal en entornos digitales.

Además, el artículo promueve una cultura de sensibilización en torno al derecho a la protección de datos personales, alineándose con la necesidad de un marco legal que permita a las personas ejercer un control efectivo sobre su información. En este sentido, refuerza la conexión con la autodeterminación informativa, resaltando que la educación digital no solo empodera a los individuos, sino que también contribuye a una mejor gobernanza de los datos en un entorno tecnológico en constante evolución.

1.3. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

La Ley Orgánica de Protección de Datos Personales de Ecuador, aprobada en 2021, establece un marco normativo integral para la salvaguarda de los datos personales de los ciudadanos, asegurando su protección frente a posibles usos indebidos o abusivos. Además de garantizar el derecho de los ecuatorianos a decidir sobre la recopilación, almacenamiento y difusión de su información. Los principios rectores de la ley incluyen la licitud, la transparencia,

la minimización de datos y la limitación del propósito, con el objetivo de asegurar que los datos solo sean procesados cuando sea estrictamente necesario y bajo condiciones claras y justas. De igual manera, establece los derechos de los titulares de los datos, como el acceso, rectificación, cancelación y oposición, permitiendo a las personas ejercer control sobre su información. Esto se extiende a las entidades extranjeras que manejen datos de residentes ecuatorianos, lo que refuerza la protección en un contexto globalizado, donde la transferencia de datos puede cruzar fronteras fácilmente. Esta normativa constituye un paso fundamental en el fortalecimiento de la protección de la privacidad y el respeto de los derechos humanos en el país, alineándose con las mejores prácticas internacionales en materia de protección de datos personales.

La promulgación de la Ley de Protección de Datos Personales en mayo de 2021 establece un marco jurídico que exige a todas las organizaciones, sin importar su tamaño o actividad económica, un análisis detallado del manejo de los datos personales bajo su responsabilidad. Para Luis Ponce es indispensable que las entidades identifiquen claramente qué datos están tratando, los medios utilizados para almacenarlos y las prácticas asociadas a su manejo, con el objetivo de garantizar que dichas actividades cumplan con los principios y disposiciones legales establecidos en la normativa (PwC Ecuador, 2021). Además, cada organización debe personalizar sus procesos de tratamiento de datos en función de su estructura y sector, para desarrollar una estrategia adecuada que asegure la implementación efectiva de esta ley. Esto requiere un diagnóstico exhaustivo de la situación actual de la entidad, que permita no solo evaluar su grado de cumplimiento normativo, sino también garantizar la seguridad y protección de los datos personales en su posesión. Este enfoque

preventivo y proactivo resulta esencial para evitar vulneraciones de derechos y para fomentar una cultura de respeto hacia la privacidad y la autodeterminación informativa.

Los principios establecidos en el artículo 10 de la Ley Orgánica de Protección de Datos Personales constituyen el eje fundamental que regula el tratamiento de datos personales en el Ecuador. Estos principios buscan garantizar la protección de los derechos de los titulares, promoviendo un manejo de la información que sea justo, seguro y conforme a la normativa vigente. Cada principio establece directrices claras sobre cómo deben gestionarse los datos, subrayando la necesidad de transparencia, proporcionalidad y responsabilidad en todas las etapas del tratamiento de la información personal (Asamblea Nacional del Ecuador, 2021). El principio de juridicidad asegura que el manejo de los datos se realice en estricto cumplimiento de las disposiciones constitucionales, legales e internacionales, reforzando así la legitimidad del tratamiento. A su vez, principios como la lealtad y la transparencia destacan la importancia de que los titulares comprendan cómo se recogen y usan sus datos, promoviendo una relación de confianza entre las personas y los responsables del tratamiento. El principio de finalidad limita el uso de los datos exclusivamente a los fines específicos y legítimos para los que fueron recopilados, evitando desvíos indebidos en su utilización.

Por otro lado, el principio de confidencialidad y el de seguridad refuerzan la obligación de proteger la información personal frente a riesgos y accesos no autorizados. Asimismo, la responsabilidad proactiva y demostrada establece que los responsables del tratamiento deben implementar medidas concretas para garantizar el cumplimiento de la ley, evidenciando un enfoque preventivo y no

solo reactivo. Finalmente, el principio de aplicación favorable al titular asegura que, en caso de duda, las disposiciones legales serán interpretadas de manera que beneficien los derechos del titular de los datos. En conjunto, estos principios no solo estructuran el marco normativo para el tratamiento de datos personales, sino que también establecen un estándar ético y técnico que refuerza la protección de la información en una sociedad donde los datos personales son cada vez más valiosos. La adecuada aplicación de estos principios será fundamental para garantizar el respeto a los derechos de las personas y promover una cultura de protección de datos en el país.

1.4. DERECHO A LA EDUCACIÓN DIGITAL

Las declaraciones de la directora nacional del Registro de Datos Públicos (Dinardap) subrayan la relación intrínseca entre los derechos digitales y la educación digital, destacando su papel fundamental para garantizar una protección efectiva de los datos personales. Para (Ponce, 2023), la educación digital, según lo señalado, no solo aborda aspectos técnicos como la seguridad en el manejo de contraseñas, sino también el empoderamiento de los ciudadanos para exigir la corrección de errores en las bases de datos y ejercer sus derechos frente al tratamiento indebido de su información personal. Esto enfatiza la importancia de un enfoque preventivo y proactivo en el manejo de los datos personales. El Proyecto de Ley de Protección de Datos Personales reconoce que la educación digital debe iniciarse desde edades tempranas y abarcar también a los adultos, quienes tienen la responsabilidad de guiar a las generaciones más jóvenes en este ámbito. Además, la normativa establece una obligación para las empresas de capacitar a su personal, reforzando así una

cultura de seguridad y protección de datos que va más allá del cumplimiento normativo, promoviendo prácticas responsables dentro de las organizaciones.

El artículo 23 de la Ley Orgánica de Protección de Datos Personales reconoce el derecho a la educación digital como una herramienta fundamental para enfrentar los desafíos de la sociedad digital contemporánea. Este derecho garantiza que todas las personas tengan acceso a conocimientos y habilidades relacionadas con el uso adecuado y seguro de las tecnologías de la información y comunicación (Asamblea Nacional del Ecuador, 2021). Al vincularlo con principios como la dignidad humana, la privacidad y la protección de datos, se refuerza la idea de que la educación digital es un pilar esencial para el ejercicio pleno de los derechos fundamentales en entornos tecnológicos. El carácter inclusivo de este derecho, particularmente en relación con personas con necesidades educativas especiales, demuestra un compromiso con la equidad y la reducción de brechas digitales. Esto es crucial en un mundo donde la exclusión tecnológica puede perpetuar desigualdades sociales. Al establecer la obligación del sistema educativo nacional, incluyendo la educación superior, de garantizar la enseñanza de estas competencias tanto a estudiantes como a docentes, se reconoce la importancia de una preparación integral y transversal para enfrentar los retos de la era digital.

Además, al abordar temas clave como la autodeterminación informativa, la ciudadanía digital y la protección de datos personales, el artículo no solo fomenta el acceso equitativo a las tecnologías, sino que también promueve la construcción de una cultura en la que los derechos digitales sean respetados y defendidos. Este enfoque integral, que combina la promoción de la inclusión digital con la responsabilidad individual y colectiva. Al mismo tiempo, fortalece

los principios de transparencia, seguridad y rendición de cuentas en el uso de tecnologías y datos personales. Con ello, no solo se contribuye a una sociedad digital más ética y equitativa, sino que también se crea un entorno en el que las personas son conscientes de sus derechos, las implicaciones de compartir información en línea y el impacto de las decisiones tecnológicas en su vida privada. Este tipo de educación y concienciación es crucial para que los ciudadanos puedan tomar decisiones informadas, proteger su identidad y contribuir a la creación de un ecosistema digital que valore la privacidad como un derecho fundamental.

1.5. REGISTRO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

El Registro Nacional de Protección de Datos Personales, establecido en el artículo 51 de la Ley Orgánica de Protección de Datos Personales, es una herramienta clave para garantizar la transparencia y el cumplimiento de las normativas en el tratamiento de datos personales en Ecuador. Su propósito principal es recopilar y mantener actualizada la información relacionada con las bases de datos y los tratamientos de datos personales realizados por responsables y encargados, bajo la supervisión de la Autoridad de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021)

Este registro permite identificar y supervisar aspectos fundamentales del tratamiento de datos, como las características y finalidades del uso de la información, la naturaleza de los datos tratados, y los mecanismos implementados para garantizar su seguridad y protección. Asimismo, promueve la rendición de cuentas al exigir la inscripción de datos de contacto, los

destinatarios de la información, y los medios utilizados para cumplir con los principios, derechos y obligaciones establecidos en la ley.

En términos funcionales, el registro actúa como un medio de control y fiscalización por parte de la autoridad correspondiente, fomentando la transparencia y reduciendo los riesgos asociados al mal manejo de datos personales. Además, al exigir detalles como los tiempos de conservación de la información y las herramientas de seguridad aplicadas, este registro asegura que los responsables y encargados del tratamiento operen de manera diligente, cumpliendo con los estándares legales y éticos para proteger los derechos de los titulares de datos personales.

1.6. LA PRIVACIDAD EN ECUADOR

En el contexto ecuatoriano, la convergencia entre la era digital y los derechos individuales plantea un desafío crucial: la vulneración del derecho a la privacidad en un entorno digital omnipresente. Según explaya Rivera (2023). Las tecnologías de la información y comunicación han tejido una compleja red que abarca tanto las interacciones personales como las actividades laborales, haciendo del resguardo de la privacidad un elemento clave para la autodeterminación y la seguridad en línea. La rápida penetración de estas tecnologías ha generado preocupación sobre la recopilación, almacenamiento y uso de datos personales, en un ecosistema digital caracterizado por un flujo constante de información y la omnipresencia de dispositivos conectados, lo que ha difuminado las fronteras entre los espacios público y privado (Rivera, 2023)

En este panorama, los ciudadanos enfrentan retos sin precedentes para mantener el control de su información personal y su exposición en línea. Para abordar este tema, se llevó a cabo una investigación que incluyó una revisión de

fuentes académicas y la realización de una encuesta a un centenar de personas de diversos sectores, buscando profundizar en los problemas y desafíos relacionados con la privacidad en la era digital.

Esto subraya un problema crucial en la sociedad actual: la vulneración del derecho a la privacidad en el contexto de una era digital que avanza rápidamente. Según lo planteado, la tecnología ha transformado profundamente la interacción entre los individuos y el entorno digital, difuminando las fronteras entre lo público y lo privado.

Esto, a su vez, ha generado retos significativos para la autodeterminación informativa y la seguridad de los datos personales. Aunque se menciona la importancia de este problema en la sociedad ecuatoriana, sería enriquecedor vincularlo directamente con normativas como la Ley Orgánica de Protección de Datos Personales, lo que permitiría contextualizar las amenazas dentro de un marco jurídico que busca proteger estos derechos fundamentales.

Por otra parte, se resalta el uso de métodos empíricos, como encuestas representativas, para explorar las percepciones de los ciudadanos sobre la privacidad digital. Este enfoque es valioso, ya que proporciona una base realista y contextualizada para el análisis. No obstante, se advierte la ausencia de un desarrollo detallado de los hallazgos obtenidos en dichas encuestas.

CAPITULO II

2.1. LA RESPONSABILIDAD LEGAL DE LAS EMPRESAS

Es responsabilidad primordial de las empresas garantizar la protección de los datos personales que recaban, almacenan y procesan. Según las investigaciones de (Meraz, 2018), las empresas deben actuar como custodios confiables de la información privada de sus clientes, empleados y demás interesados. Este rol implica adoptar un enfoque proactivo y cumplir rigurosamente con las normativas de protección de datos vigentes. Al hacerlo, las organizaciones no solo evitan sanciones legales y daños a su reputación, sino que también construyen una relación de confianza sólida con los usuarios, lo cual es fundamental para el éxito a largo plazo de cualquier negocio. Por lo tanto, la protección de datos debe ser considerada como una inversión estratégica, y no meramente como un cumplimiento normativo.

En el marco del principio de responsabilidad en la protección de datos personales, se establece que los responsables y encargados del tratamiento deben implementar medidas técnicas y organizacionales efectivas que garanticen el cumplimiento de los principios de privacidad y seguridad. Como expone la (Organización de Estados Americanos, 2023), estas medidas, que incluyen auditorías y actualizaciones periódicas, deben permitir a las empresas demostrar su conformidad y cooperar con las autoridades cuando sea necesario. Asimismo, los responsables de datos tienen la obligación de actuar como "buenos custodios" de la información que gestionan

Este principio enfatiza que la responsabilidad no solo es una exigencia normativa, sino también un compromiso ético y operativo que deben asumir las empresas. La capacidad de demostrar cumplimiento en el tratamiento de datos

personales implica que las organizaciones deben ser proactivas en la implementación de medidas que vayan más allá del mínimo requerido por la ley, como auditorías constantes y revisiones periódicas de sus prácticas.

En Ecuador, donde la Ley de Protección de Datos Personales que se encuentra consolidada. Estas revisiones previamente mencionadas aún tienen defectos, por lo que este principio debería servir como base para que las empresas adopten un enfoque preventivo. Esto incluye no solo cumplir con las disposiciones legales, sino también adaptarlas a sus operaciones internas, promoviendo una cultura de transparencia y responsabilidad.

Para este sistema de cumplimiento es necesario el establecimiento de metas claras para la protección de la privacidad, tal como señala la (Organización de Estados Americanos, 2023), permite a las empresas determinar las estrategias más adecuadas para alcanzar dichas metas en función de sus particularidades. Por ejemplo, una empresa tecnológica podría priorizar la implementación de sistemas avanzados de encriptación, mientras que una institución financiera podría centrarse en controles de acceso más estrictos y capacitaciones internas.

Además, el principio destaca la importancia de seleccionar socios o encargados del tratamiento que puedan garantizar un nivel adecuado de protección, lo cual subraya la necesidad de criterios estrictos en la tercerización de servicios relacionados con datos personales. Esto es crucial en un entorno digital globalizado, donde las cadenas de tratamiento de datos pueden involucrar a múltiples actores en diferentes jurisdicciones.

Para el contexto ecuatoriano, este enfoque podría inspirar un sistema más sólido de regulación y supervisión, con la Autoridad de Protección de Datos Personales desempeñando un papel central en la evaluación del cumplimiento. Además, El principio número trece de la (Organización de Estados Americanos, 2023), apoya que las empresas deben ser incentivadas a incorporar políticas internas de autoevaluación y auditoría que refuercen su responsabilidad frente a los titulares de datos

Finalmente, esta unión de los principios diez y trece de la OEA nos recuerdan que las empresas tienen un papel dual: por un lado, como sujetos regulados que deben cumplir con las leyes, y por otro, como agentes éticos que deben ser capaces de proteger los derechos de las personas, incluso en contextos donde las normativas puedan ser insuficientes. La adopción de este estándar permitiría no solo proteger a los ciudadanos, sino también fomentar la confianza en el ecosistema digital, fortaleciendo la economía digital en el país.

2.1.1. DE LA RESPONSABILIDAD PROACTIVA

Establece la ley Orgánica de Protección de Datos personales en su artículo 52:

> "Autorregulación. -Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de conducta, certificaciones, sellos y marcas de protección, cláusulas tipo, sin que esto constituya eximente de la responsabilidad de cumplir con las disposiciones de la presente Ley, su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia." (Asamblea Nacional del Ecuador, 2021)

El artículo 52 de la Ley Orgánica de Protección de Datos Personales introduce el principio de responsabilidad proactiva mediante el concepto de autorregulación. Este principio permite que los responsables y encargados del

tratamiento de datos personales adopten medidas adicionales, como códigos de conducta, certificaciones y sellos de protección, que refuercen las buenas prácticas en la gestión de datos. Sin embargo, es crucial señalar que estas herramientas no eximen a los responsables de cumplir con las disposiciones legales establecidas, incluyendo las directrices y regulaciones emitidas por la Autoridad de Protección de Datos Personales.

Este enfoque refleja un avance en la gobernanza de datos personales, incentivando una cultura de cumplimiento más allá de las obligaciones mínimas legales. La posibilidad de autorregulación fomenta la implementación de estándares elevados de protección, lo que podría fortalecer la confianza de los ciudadanos en el manejo de su información personal. No obstante, es fundamental que la Autoridad de Protección de Datos supervise de manera activa estos mecanismos voluntarios, para garantizar que no se utilicen como una fachada para eludir responsabilidades.

Desde una perspectiva crítica, si bien la autorregulación puede ser un mecanismo eficaz, también puede generar desafíos. Por un lado, puede contribuir a la construcción de un entorno digital más seguro. Por otro, existe el riesgo de que la implementación de códigos y certificaciones se limite a cumplir requisitos formales, sin que se traduzca en un cambio real en la cultura organizacional. Para evitar esto, es esencial que las normativas acompañen y refuercen estas iniciativas con mecanismos de control y sanción efectivos.

2.2. PRIVACIDAD Y SEGURIDAD DE DATOS EN EL CONTEXTO DIGITAL

Según ha delimitado la Angela María Cristancho como directora de la Fundación Fepropaz: La privacidad de los datos permite a las personas ejercer control sobre la información que se recopila sobre ellas, definiendo cómo se

utiliza y con quién se comparte, mientras que la seguridad de los datos busca proteger la integridad, confidencialidad y disponibilidad de esta información mediante medidas técnicas y organizativas destinadas a prevenir accesos no autorizados y ciber amenazas (Cristancho, 2023)

La protección de la privacidad y la seguridad de los datos es un pilar fundamental en la era digital, pues aborda el resguardo de la información personal y sensible en sistemas tecnológicos interconectados. Según se plantea, estos conceptos, aunque relacionados, representan dimensiones complementarias en el manejo de la información en línea. La privacidad de los datos otorga a los individuos el control sobre la información que se recopila sobre ellos, asegurando su dignidad y autonomía mediante mecanismos de transparencia y consentimiento informado. Por su parte, la seguridad de los datos garantiza la confidencialidad e integridad de la información almacenada, implementando medidas preventivas contra accesos no autorizados y ciber amenazas.

Cristancho (2023) define la privacidad de datos como el derecho de los individuos a controlar la información personal que se recopila, su uso y con quién se comparte. Paralelamente, la seguridad de datos se centra en proteger la integridad, confidencialidad y disponibilidad de la información almacenada a través de medidas técnicas y organizativas. Este análisis resalta la interdependencia de ambos conceptos, donde la privacidad requiere la seguridad para su protección, y la seguridad debe respaldar los derechos de privacidad de los usuarios

Desde una perspectiva crítica, es evidente que la creciente conectividad y las tecnologías de análisis masivo exigen un enfoque robusto y ético en la

gestión de datos personales. La afirmación de que garantizar una adecuada protección de la privacidad y la seguridad es esencial para fomentar la confianza de los usuarios en la tecnología señala con precisión que el desarrollo tecnológico debe ir acompañado de principios claros que prioricen los derechos individuales. Este enfoque es indispensable para evitar escenarios de vigilancia masiva o mal uso de la información, promoviendo un entorno digital en el que prevalezca la equidad y la protección de los derechos fundamentales.

En el ámbito de la protección de datos, las empresas deben adoptar un enfoque técnico que priorice herramientas como el cifrado para garantizar la confidencialidad de la información, la autenticación robusta para validar el acceso de usuarios legítimos, controles de acceso que limiten la exposición de datos y protocolos seguros en la capa de red que protejan la información durante su transmisión.

El enfoque técnico descrito no solo representa un conjunto de prácticas deseables, sino un estándar mínimo que las empresas deben adoptar para garantizar la privacidad y seguridad de los datos personales que manejan. Estas medidas no son opcionales en un entorno digital donde las amenazas a la información son constantes y cada vez más sofisticadas.

El cifrado, por ejemplo, debería ser una práctica habitual para proteger datos sensibles almacenados y en tránsito. Las empresas que manejan datos personales, desde grandes corporaciones hasta pequeñas entidades, tienen la responsabilidad de implementar soluciones criptográficas modernas y mantenerlas actualizadas para evitar brechas de seguridad.

Asimismo, la autenticación robusta, como el uso de autenticación de dos factores (2FA), debe ser una norma, no solo para los usuarios finales, sino también para los empleados que manejan sistemas críticos. Este enfoque proactivo reduce significativamente el riesgo de accesos no autorizados, incluso si las contraseñas son comprometidas.

El control de acceso y la segmentación de privilegios deben integrarse en las políticas organizativas para evitar que empleados o sistemas no autorizados accedan a información innecesaria. Esto fomenta un modelo de seguridad de "menor privilegio", que es vital para minimizar riesgos.

Finalmente, la protección en la capa de red mediante protocolos como HTTPS y el uso de VPNs es indispensable, especialmente para empresas que procesan datos a través de redes públicas. Esto no solo protege la información de ataques de interceptación, sino que también refuerza la confianza de los usuarios al garantizar que sus datos no serán vulnerados.

Adoptar estas medidas técnicas no solo protege a las empresas de las consecuencias legales de un incumplimiento, sino que también fortalece la confianza de los usuarios y consolida la reputación corporativa. En este sentido, la responsabilidad de implementar estos enfoques recae no solo en los departamentos técnicos, sino también en la alta gerencia, que debe garantizar los recursos necesarios para una implementación efectiva y sostenible.

2.3. RESPONSABILIDAD CIVIL RESPECTO A DATOS PERSONALES

En el contexto de la responsabilidad civil empresarial frente a los clientes y usuarios, cuando se produce un ciberataque que interrumpe la prestación de un servicio esencial como el suministro eléctrico, las empresas están obligadas

a garantizar que este sea entregado con calidad y sin interrupciones. De acuerdo con la (ENATIC, 2023), cuando una interrupción en el servicio causa daños a los consumidores finales, estos tienen el derecho de exigir indemnizaciones bajo el argumento de incumplimiento contractual, siempre que logren demostrar la relación de causalidad entre el daño sufrido y la falla en el servicio. Por su parte, las empresas solo podrán exonerarse de responsabilidad si demuestran que actuaron con la debida diligencia en la implementación de medidas de seguridad técnicas adecuadas y que el evento fue completamente imprevisible e inevitable.

Este enfoque en la legislación española resalta la necesidad de un marco normativo robusto que regule la responsabilidad civil de las empresas frente a los consumidores en casos de ciberataques. En Ecuador, la falta de una regulación específica y detallada en esta materia podría llevar a que los consumidores queden en una situación de vulnerabilidad ante interrupciones de servicios esenciales causadas por fallos en la seguridad informática de las empresas.

El análisis del sistema español pone de manifiesto la importancia de establecer un balance entre los derechos de los consumidores y las garantías de las empresas. Por un lado, los consumidores tienen la carga de demostrar que el daño sufrido se deriva directamente del fallo en el servicio. Por otro lado, las empresas deben probar que adoptaron todas las medidas necesarias para prevenir o mitigar riesgos, aplicando un estándar de diligencia razonable.

En Ecuador, la implementación de un sistema similar implicaría la necesidad de regular con claridad los estándares de seguridad informática que deben cumplir las empresas prestadoras de servicios esenciales, así como los mecanismos para que los consumidores puedan reclamar indemnizaciones.

Además, sería necesario incorporar disposiciones que exijan a las empresas la adopción de medidas preventivas, y que sancionen la negligencia en la implementación de dichas medidas. Un marco de responsabilidad civil adaptado a la realidad ecuatoriana no solo protegería a los consumidores, sino que también incentivaría a las empresas a invertir en ciberseguridad, promoviendo una cultura de prevención y mejorando la confianza en los servicios digitales en el país.

CAPITULO III

3.1. VULNERACIÓN A LOS DATOS PERSONALES

Las vulneraciones de seguridad en los datos personales representan uno de los mayores riesgos en la era digital, pues exponen la confidencialidad, integridad y disponibilidad de la información de los individuos. La (Organización de Estados Americanos, 2023) en su principio seis, señala que Estas vulneraciones pueden ser consecuencia de brechas en la seguridad técnica, errores humanos o accesos no autorizados que resultan en pérdidas, alteraciones, divulgaciones indebidas o interrupciones en el acceso a la información. Ante estos riesgos, los principios de seguridad subrayan la importancia de implementar medidas técnicas y organizativas adecuadas que no solo prevengan estas situaciones, sino que también permitan detectarlas y mitigarlas oportunamente.

Las vulneraciones de seguridad de los datos personales plantean desafíos significativos para las organizaciones, dado que comprometen no solo la información sensible de los individuos, sino también la confianza que estos depositan en las instituciones responsables de su tratamiento. Estas situaciones, que incluyen desde el acceso no autorizado hasta la divulgación accidental de información, afectan de manera directa la percepción pública sobre la capacidad de las entidades para gestionar adecuadamente los datos. Este fenómeno, cada vez más frecuente debido al incremento de la interconectividad digital y la sofisticación de los ciberataques, revela fallas sistémicas en las políticas de protección y gestión de datos. La falta de medidas preventivas adecuadas no solo expone vulnerabilidades, sino que también perpetúa un entorno de riesgo que puede ser aprovechado por actores malintencionados.

Desde un punto de vista técnico, la responsabilidad de las organizaciones radica en adoptar medidas preventivas robustas, como sistemas avanzados de encriptación, controles de acceso restringidos y monitoreo continuo de las redes. Estas herramientas deben configurarse de manera eficiente y mantenerse actualizadas frente a las nuevas amenazas tecnológicas que surgen constantemente. La implementación de inteligencia artificial y aprendizaje automático para detectar patrones anómalos en el tráfico de datos puede ser una estrategia adicional para prevenir incidentes. Sin embargo, estas acciones deben ser acompañadas por protocolos claros de respuesta ante incidentes, que permitan actuar de manera inmediata y eficaz cuando una brecha de seguridad sea detectada. Este enfoque incluye la creación de equipos de respuesta rápida, simulacros de gestión de crisis y una comunicación efectiva con las partes afectadas para mitigar el impacto de los incidentes.

No obstante, el problema no se limita al ámbito tecnológico. Muchas vulneraciones tienen su origen en errores humanos, como la falta de capacitación del personal o la aplicación inconsistente de las políticas de seguridad. Como señala (Rosero, 2021), las contraseñas débiles, el phishing y el mal manejo de la información confidencial son ejemplos de prácticas deficientes que pueden comprometer la seguridad. En este sentido, los principios de seguridad enfatizan la necesidad de complementar las herramientas técnicas con medidas organizativas, como programas de formación continua, simulaciones periódicas de ataques y auditorías regulares, para garantizar que todos los niveles de la organización estén alineados con los estándares de protección de datos. Estas medidas no solo reducen el riesgo de incidentes, sino

que también fomentan una cultura de seguridad dentro de las organizaciones, donde cada empleado entiende su rol en la protección de los datos personales.

En el contexto ecuatoriano, estas vulneraciones adquieren una dimensión crítica debido a la reciente implementación de la Ley de Protección de Datos Personales, que aún enfrenta desafíos en términos de regulación y supervisión efectiva. El marco normativo establece obligaciones claras, pero su éxito depende en gran medida de la capacidad de las autoridades para fiscalizar su cumplimiento y de la disposición de las empresas para incorporar buenas prácticas en su gestión. Es imperativo que las empresas y entidades públicas no solo cumplan con los requisitos legales, sino que desarrollen una cultura de seguridad que priorice la protección de la información personal como un derecho fundamental. Este compromiso requiere inversión en infraestructura tecnológica, capacitación y el establecimiento de líneas de comunicación directa con los titulares de los datos, quienes deben ser informados y empoderados respecto a sus derechos.

Además, el impacto de las vulneraciones trasciende lo individual, afectando sectores enteros de la economía digital. Una violación de datos puede provocar pérdidas económicas considerables, sanciones legales y un daño reputacional irreparable para las organizaciones involucradas. Estas consecuencias no solo afectan a las empresas de manera inmediata, sino que también generan un efecto cascada en el mercado, donde la pérdida de confianza por parte de los consumidores y socios comerciales puede tener repercusiones a largo plazo. En este sentido, adoptar un enfoque proactivo y alineado con los principios de seguridad no solo es una obligación ética y legal,

sino también una estrategia clave para garantizar la sostenibilidad en el entorno digital. Fomentar una colaboración activa entre empresas, gobiernos y expertos en ciberseguridad es esencial para fortalecer las barreras frente a las amenazas y construir un ecosistema digital más seguro y resiliente.

3.2. PROTOCOLO DE DENUNCIAS Y SOLICITUDES EN PROTECCIÓN DE DATOS PERSONALES

El análisis de (Unda, 2024), integrante de Meythaler & Zambrano Abogados, detalla el procedimiento para presentar denuncias y solicitudes relacionadas con la protección de datos personales en Ecuador. Dicho análisis subraya la relevancia de la Ley Orgánica de Protección de Datos Personales (LOPDP) y el papel de la Superintendencia de Protección de Datos Personales (SPDP) en la recepción y gestión de estas denuncias.

Desde una perspectiva jurídica, es fundamental reconocer que la LOPDP establece un marco normativo robusto para la protección de los datos personales en Ecuador. La creación de la SPDP como entidad encargada de supervisar y garantizar el cumplimiento de esta ley representa un avance significativo en la tutela de los derechos de los titulares de datos. Sin embargo, la eficacia de este marco legal depende en gran medida de la accesibilidad y claridad de los procedimientos establecidos para que los ciudadanos puedan ejercer sus derechos.

El artículo menciona que la SPDP ha implementado un formulario para la recepción de denuncias, disponible en su sitio web oficial. Esta iniciativa es loable, ya que facilita a los ciudadanos la presentación de quejas por posibles incumplimientos en el tratamiento de sus datos personales. No obstante, es crucial que este formulario sea de fácil acceso y comprensión para garantizar su

uso efectivo por parte de la población en general. Además, se destaca la importancia de que las instituciones, tanto públicas como privadas, desarrollen y publiquen políticas de protección de datos que sean claras y accesibles. Estas políticas deben detallar aspectos como las finalidades del tratamiento de los datos, los derechos de los titulares y las medidas de seguridad implementadas para proteger la información. La transparencia en estas prácticas no solo cumple con las exigencias legales, sino que también fortalece la confianza de los ciudadanos en el manejo de sus datos por parte de las organizaciones.

Es pertinente señalar que, aunque la SPDP ha lanzado su página web oficial con herramientas clave para la gestión de datos, como el registro de delegados de protección de datos y la recepción de denuncias, la efectividad de estas herramientas dependerá de su correcta implementación y de la capacitación tanto de los responsables del tratamiento de datos como de los titulares. La formación y concienciación en materia de protección de datos son esenciales para asegurar el cumplimiento de la normativa y la protección efectiva de los derechos de los ciudadanos.

Un aspecto relevante tratado en el artículo es la facultad de la SPDP para imponer sanciones ante incumplimientos de la normativa de protección de datos personales. La posibilidad de aplicar sanciones administrativas representa un mecanismo clave para disuadir prácticas inadecuadas en el tratamiento de datos personales. Sin embargo, la efectividad de estas sanciones dependerá de su correcta aplicación y del grado de fiscalización que realmente pueda ejercer la SPDP. En este sentido, resulta fundamental garantizar que el proceso sancionador sea transparente y que se respeten los principios del debido proceso y la proporcionalidad en la imposición de multas o medidas correctivas.

El artículo también menciona el derecho de los ciudadanos a presentar solicitudes para ejercer sus derechos en materia de datos personales, como el acceso, rectificación, cancelación y oposición. La posibilidad de exigir la corrección o eliminación de información inexacta es esencial para garantizar la autodeterminación informativa. No obstante, la eficacia de estos derechos dependerá de la respuesta oportuna y efectiva de las entidades responsables del tratamiento de datos. En este punto, sería pertinente evaluar si la normativa vigente establece plazos y procedimientos claros para la atención de estas solicitudes y si existen mecanismos adecuados de seguimiento y control para evitar dilaciones o negativas injustificadas.

Otro punto abordado es la importancia de contar con delegados de protección de datos en las instituciones que manejan información personal. La designación de estos delegados es una estrategia adecuada para asegurar el cumplimiento de la normativa y fomentar una cultura de protección de datos dentro de las organizaciones. Sin embargo, su eficacia estará condicionada a la capacitación y autonomía que realmente posean para ejercer sus funciones. Si bien la ley contempla esta figura, es necesario analizar si existen criterios claros para su nombramiento y si se han implementado programas de formación que garanticen su idoneidad en la materia.

Finalmente, el artículo resalta la obligación de las instituciones de notificar incidentes de seguridad relacionados con la protección de datos. Esta medida es crucial para mitigar riesgos y permitir que los titulares de datos tomen medidas adecuadas en caso de una posible vulneración de su información. No obstante, un análisis crítico exige cuestionarse hasta qué punto las entidades cumplen con esta obligación de manera efectiva y si existen sanciones suficientes para

disuadir omisiones en la notificación de estos incidentes. La transparencia en la gestión de brechas de seguridad es un factor determinante en la protección de datos personales, por lo que resulta fundamental que este mecanismo se implemente de manera rigurosa y eficaz. En síntesis, el artículo ofrece un panorama detallado sobre los mecanismos de protección de datos en Ecuador, resaltando avances normativos y desafíos pendientes. Si bien la LOPDP y la SPDP constituyen un progreso significativo, su efectividad dependerá de la aplicación real de los procedimientos establecidos y de la promoción de una cultura de cumplimiento.

3.3. APLICACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES RESPECTO A LA RESPONSABILIDAD LEGAL DE LAS EMPRESAS

La adecuada implementación de la Ley Orgánica de Protección de Datos Personales y el cumplimiento proactivo de las empresas en la adopción de medidas de seguridad cibernética no solo reducen significativamente las vulneraciones de datos personales, sino que también fortalecen la protección de los derechos de los ciudadanos y fomentan la confianza en el entorno digital ecuatoriano. En un contexto donde la digitalización de los servicios y el manejo masivo de información personal son cada vez más frecuentes, las empresas tienen la obligación legal y ética de garantizar la privacidad y seguridad de los datos que administran. El incumplimiento de estas normativas no solo puede derivar en sanciones legales y económicas, sino que también puede afectar la reputación corporativa y generar pérdida de credibilidad ante clientes y socios estratégicos.

En este sentido, la responsabilidad legal de las empresas en materia de protección de datos personales no es solo un deber normativo, sino un

compromiso con la confianza y la transparencia. Es un pacto silencioso entre quien confía su información y quien la resguarda, un lazo de seguridad tejido con políticas claras, formación constante y tecnologías que vigilan como centinelas incansables. No basta con reaccionar ante la tormenta, es preciso anticiparse al viento, erigir murallas contra la incertidumbre y blindar cada dato como si fuese un tesoro irremplazable.

Cumplir con esta misión es más que acatar una ley: es honrar el derecho de cada persona a la privacidad, es proteger su historia y su identidad en el vasto océano digital. Porque en cada cifra, en cada nombre, en cada fragmento de información, late una vida que merece respeto y cuidado. Solo así, con una gestión ética y responsable, podrá florecer un ecosistema digital donde la confianza no sea un anhelo, sino una certeza; donde los muros de protección no sean fríos obstáculos, sino puentes hacia un futuro más seguro y justo.

CONCLUSIONES

Se concluye que: La protección de datos personales en Ecuador ha avanzado con la Ley Orgánica de Protección de Datos Personales, pero aún existen deficiencias en su aplicación por parte de las empresas. Aunque la normativa establece principios claros, muchas organizaciones no cumplen con los estándares mínimos exigidos, lo que deja a los ciudadanos expuestos a riesgos. Además, la falta de una supervisión estricta ha permitido que varias entidades manejen información sin las medidas adecuadas de seguridad.

Se concluye que: Muchas empresas no aplican medidas de seguridad adecuadas, lo que incrementa el riesgo de violaciones de datos personales. La falta de inversiones en herramientas de protección, como cifrado y autenticación robusta, facilita el acceso no autorizado a la información sensible de los usuarios. Esto no solo afecta la privacidad de los ciudadanos, sino que también puede derivar en consecuencias legales para las organizaciones responsables.

Se concluye que: La falta de capacitación en protección de datos dentro de las organizaciones contribuye a errores humanos y vulneraciones de seguridad. Muchos incidentes de filtración de información no ocurren solo por fallas tecnológicas, sino también por desconocimiento o negligencia de los empleados al manejar datos personales. Sin una formación adecuada, los trabajadores pueden ser víctimas de ingeniería social, phishing o malas prácticas en la gestión de información sensible.

Se concluye que: Los ciudadanos no siempre están informados sobre sus derechos en cuanto a la protección de sus datos personales. Muchas personas desconocen cómo se recopila, almacena y usa su información, lo que dificulta que puedan ejercer su autodeterminación informativa. Esto genera un entorno

donde los datos pueden ser utilizados sin el consentimiento adecuado, facilitando abusos por parte de empresas y entidades públicas.

Se concluye que: Cuando ocurre una violación de datos, muchas empresas no notifican a los afectados de manera oportuna, lo que impide que tomen medidas para proteger su información. Además, la ausencia de planes de respuesta bien estructurados agrava el impacto de estos incidentes, afectando la reputación de las organizaciones y debilitando la seguridad en el ecosistema digital.

RECOMENDACIONES

Se recomienda: Fortalecer la supervisión y fiscalización del cumplimiento normativo para garantizar la correcta implementación de la ley. Para ello, la Autoridad de Protección de Datos Personales debe aumentar su capacidad de monitoreo y sanción en casos de incumplimiento. También es necesario promover auditorías regulares en las empresas para verificar su nivel de adecuación a la normativa vigente.

Se recomienda: Que las empresas adopten protocolos de seguridad más estrictos, como cifrado y autenticación de dos factores, para mitigar estos riesgos. Además, deben realizar auditorías periódicas de ciberseguridad para evaluar sus vulnerabilidades y actualizar sus sistemas. Implementar un enfoque de seguridad por diseño permitirá reducir significativamente la exposición a posibles ataques o filtraciones de datos.

Se recomienda: Implementar programas de formación continua para empleados y responsables del manejo de datos personales. Las capacitaciones deben incluir simulaciones de ciberataques, buenas prácticas en el uso de contraseñas y procedimientos para reportar incidentes. Además, se recomienda establecer protocolos internos claros para minimizar el impacto de errores humanos en la seguridad de los datos.

Se recomienda: Realizar campañas de concienciación sobre la autodeterminación informativa y los mecanismos de denuncia en caso de vulneraciones. Es clave que el Estado, junto con organismos especializados, desarrolle materiales educativos accesibles sobre la protección de datos y

seguridad digital. Además, se pueden promover talleres y plataformas interactivas para empoderar a los ciudadanos en la defensa de su privacidad

Se recomienda: Que las empresas y entidades gubernamentales desarrollen planes de respuesta a incidentes que incluyan notificación oportuna a los afectados. Estos protocolos deben establecer tiempos claros para la detección, contención y comunicación de las vulneraciones de datos. Asimismo, es recomendable la creación de equipos de respuesta a incidentes de seguridad que coordinen acciones efectivas para minimizar daños y prevenir futuros ataques.

REFERENCIAS BIBLIOGRÁFICAS

Adinolfi, G. (2007). Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental. *Cuestiones constitucionales*, 03-29.

Asamblea Nacional del Ecuador. (26 de Mayo de 2021). Ley Orgánica De Protección De Datos Personales. *Registro Oficial Suplemento 459*. Quito, Pichincha , Ecuador: Lexis.

Barahona, L., Arreaga, G., & Estrella, F. (2021). Protección de los derechos en caso de violencia intrafamiliar. *Universidad y Sociedad*, 318 - 329.

Comisión Europea. (26 de 11 de 2024). *Web Oficial de la Comisión Europea*. Obtenido de https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

Cristancho, A. (23 de Julio de 2023). *Fepropaz.com*. Obtenido de Fepropaz: https://fepropaz.com/privacidad-y-seguridad-de-datos/

ENATIC. (2023). *La Responsabilidad Legal de las Empresas Frente a un Ciberataque.* Madrid: ISMS Spain Forum.

Hernández, E., Duque, N., & Moreno, J. (2017). Big Data: una exploración de investigaciones, tecnologías y casos de aplicación. *TecnoLógica*, 15-38.

Meraz, A. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. *Revista IUS*, 293-310.

Organización de Estados Americanos. (2023). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.* New York: Secretaría General de la OEA.

Paredes, T., López, G., & Cáceres, N. (2023). Violencia intrafamiliar y medidas de protección dictadas en favor de niños y niñas mediante procesos administrativos en el Ecuador. *Ciencia Latina*, 13534-13548.

Polo, A. (2021). Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. *Revista Estudios Deusto*, 211-240.

Ponce, L. (15 de Enero de 2023). *www.Pwc.com*. Obtenido de https://www.pwc.ec/es/entrevistas-de-temas-de-interes/todo-lo-que-debes-conocer-sobre-la-proteccion-de-datos-personales.html

Rivera, Y. (2023). Vulneración del derecho a la privacidad dentro de la era digital en el Ecuador. *Polo del Conocimiento* , 982.1009.

Roldan, F. (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 Review*, 175-202.

Rosero, L. (2021). *El phishing como riesgo informático, Técnicas de mapeo en los canales electrónicos: Un mapeo sistemático.* Guayaquil: Universidad Politéncia Salesiana del Ecuador.

Unda, D. (05 de Diciembre de 2024). *https://www.meythalerzambranoabogados.com/*. Obtenido de Meythaler & Zambrano Abogados: https://www.meythalerzambranoabogados.com/post/como-presentar-denuncias-y-solicitudes-en-proteccion-de-datos-personales-en-ecuador