UNIVERSIDAD ESAN

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

CARRERA DE DERECHO CORPORATIVO

“Análisis de la eficacia normativa de la Ley de Protección de Datos Personales en el sector empresarial financiero: Propuesta de mejora del marco normativo para el fortalecimiento de la Ciberseguridad Corporativa”

Trabajo de Suficiencia Profesional presentado en satisfacción parcial de los requerimientos para obtener el Título Profesional de Abogado

AUTORES

Champi Zavaleta, Luis Alberto
Del Aguila Rodriguez, Barbara Ximena
Garcia Martinez, Andrea Felicitas
Meneses Oriundo, Yolimar Lesly

ASESOR

Camargo Roman, Mariela Isabel
ORCID N° 0009-0003-8037-6605

Lima, 2025

Informe de similitud

Trabajo de Suficiencia Profesional_Grupo 5.docx (2).pdf

INFORME DE ORIGINALIDAD

7%	14%	10%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.informatica-juridica.com Fuente de Internet	3%
2	www.researchgate.net Fuente de Internet	1%
3	docta.ucm.es Fuente de Internet	1%
4	repositorio.unjfsc.edu.pe Fuente de Internet	1%
5	hdl.handle.net Fuente de Internet	1%
6	www.camara.gov.co Fuente de Internet	1%
7	iij.ucr.ac.cr Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

Dedicatoria

A mis amados padres, Luis Alberto Champi Diaz y Mary Mabel Zavaleta Ortiz.
A mis amados abuelos, Luis Alberto y Delia.
A mi amada tía, Maria Luisa.
Y a todo ser que por mi camino ha pasado, porque no somos islas, todos nos enseñan algo.

Luis

A mi esposo que constantemente está apoyándome para ser una mejor versión de mi misma y continuar en el camino.
A mi hijo, que es mi mayor motivación para no rendirme y lograr ser su mejor ejemplo.
También, dedico esta tesis a mis ángeles, mis padres que desde el cielo me iluminan para seguir adelante con todos mis proyectos.

Bárbara

A mis amados padres, Roberto y Martha, quienes han sido mi impulso inquebrantable en cada paso de este camino. Su amor, sacrificio y apoyo incondicional me han dado la fuerza para alcanzar mis metas. A mis hijos, mi mayor motivación, porque en ellos encuentro la inspiración y el propósito para seguir creciendo y superándome cada día. Y a mi esposo, mi compañero de vida, por estar siempre a mi lado, compartiendo cada reto y cada logro con amor y paciencia.

Andrea

A Dios, por ser mi guía, por darme la sabiduría y paciencia para llegar a este momento. A mi papá, quien siempre estará en mi corazón, por su amor, sus enseñanzas y la huella que dejó en mi vida. Aunque ya no esté físicamente, sigue siendo mi mayor motivación. A mi mamá, que es mi gran soporte y ejemplo de amor incondicional. Agradezco siempre el apoyo que me das, tus sacrificios y por estar siempre conmigo. Este trabajo es el reflejo de su amor y comprensión.

Yolimar

ÍNDICE DE CONTENIDO

RESUMEN

Este trabajo que lleva como título “Análisis de la eficacia normativa de la Ley de Protección de Datos Personales en el sector empresarial financiero: Propuesta de mejora del marco normativo para el fortalecimiento de la Ciberseguridad Corporativa” busca dar una contribución en la aplicación de la legislación de Protección de Datos Personales para que de esta forma se pueda prevenir la ocurrencia de ciberataques a las empresas del sector financiero, para lo que se analizan los casos más relevantes en el Perú, junto con un ejemplo extranjero. Con el avance de las nuevas tecnologías, la protección de datos personales se ha convertido en una prioridad para todas las empresas y entidades que manejan bancos de datos, considerando como uno de los sectores más importantes y sensibles al de la banca y finanzas. Por tanto, este trabajo busca analizar en sede nacional la legislación referente a la Protección de Datos Personales, la cual consta en la Ley N° 29733, observando así qué tan eficaz es esta norma para alcanzar sus fines de resguardo de los derechos fundamentales.

PALABRAS CLAVES:

Protección de datos, ciberseguridad, entidades financieras, privacidad, ciberataque.

ABSTRACT

This work, entitled "Analysis of the regulatory effectiveness of the Personal Data Protection Law in the financial business sector: Proposal for improvement of the Legal Framework for the strengthening of Corporate Cybersecurity" seeks to contribute to the application of the Personal Data Protection legislation so that the occurrence of cyberattacks on companies in the financial sector can be prevented, for which the most relevant cases in Peru are analyzed, along with a foreign example. With the advancement of new technologies, the protection of personal data has become a priority for all companies and entities that manage databases, considering banking and finance as one of the most important and sensitive sectors. Therefore, this work seeks to analyze at the national level the legislation regarding the Protection of Personal Data, which is contained in Law No. 297333, thus observing how efficient this regulation is in achieving its objectives of safeguarding fundamental rights.

KEY WORDS:

Data protection, cybersecurity, financial institutions, privacy, cyberattack.

CAPÍTULO I: INTRODUCCIÓN

1.1. Descripción de la realidad problemática

Actualmente, la protección de datos personales se ha transformado en una prioridad global, sobre todo en sectores financieros, donde la manipulación y la seguridad de la información de los clientes son esenciales. En el Perú, la Ley de Protección de Datos Personales (Ley 29733), constituye un marco normativo para la protección de los datos personales de los individuos. No obstante, pese a ser promulgada, la implementación de esta norma en el sector empresarial financiero aún presenta distintos desafíos que afectan su eficacia.

El sector empresarial financiero en Perú, manipula impensables volúmenes de datos sensibles, los cuales se ven expuestos a ciertos riesgos asociados a la ciberseguridad. El robo de datos, amenazas cibernéticas o el acceso no autorizado a datos confidenciales, ponen en peligro la seguridad de la información personal de los clientes. Es así que la Ley 29733 tiene el objetivo de mitigar estos riesgos pero su eficacia va depender de la correcta implementación dentro de los sistemas de ciberseguridad de las entidades financieras.

El problema principal es que existe una brecha entre lo dispuesto por la Ley 29733 y su aplicación práctica en los sistemas de ciberseguridad de las empresas financieras. A pesar de la presencia de esta norma, muchas empresas y organizaciones no están cumpliendo con los requisitos establecidos o no cuentan con la capacidad técnicas para aplicar correctamente las medidas de protección, generando vulnerabilidades provechosas para atacantes cibernéticos, exponiendo datos sensibles de los clientes para un posible mal uso.

Por otro lado, los factores normativos que restringen la eficacia de la Ley de Protección de Datos en diferentes tramos del sector financiero empresarial, como la inadecuada capacitación al personal, falta de recursos técnicos, sanciones efectivas, contribuyen a la deficiencia en la salvaguarda de la información personal. Esto representa un peligro tanto para los usuarios como para las propias empresas, quienes podrían afrontar serias consecuencias legales y reputacionales por no cumplir con la normativa.

Por último, una inadecuada implementación de la ley podría desencadenar consecuencias jurídicas y operativas. Las empresas que no priorizan la protección adecuada de los datos personales de sus clientes podrían ser sancionados con multas, enfrentar demandas, perder la confianza de sus clientes, afectando gravemente su reputación y competitividad en el mercado.

1.2. Problemas de investigación

1.2.1. Problema general

¿De qué forma la Ley de Protección de Datos Personales en el Perú es eficaz para garantizar la protección de datos personales en los sistemas de ciberseguridad del sector empresarial financiero?

1.2.2. Problemas específicos

1. ¿Cuáles son las brechas entre el marco normativo de la Ley 29733 y su implementación práctica en los sistemas de ciberseguridad empresarial?

2. ¿Qué factores normativos limitan la eficacia de la Ley 29733 en la protección de datos personales en diferentes segmentos empresariales?

3. ¿Cuáles son las consecuencias jurídicas y operativas del incumplimiento de la Ley 29733 en la seguridad de los datos personales en el ámbito empresarial financiero?

1.3. Objetivos de investigación

1.3.1. Objetivo general

Analizar la eficacia de la Ley 29733 en la protección de datos personales a través de los sistemas de ciberseguridad en el sector empresarial financiero.

1.3.2. Objetivos específicos

1. Identificar y analizar las brechas existentes entre las disposiciones de la Ley 29733 y su implementación práctica en los sistemas de ciberseguridad empresarial.

2. Evaluar los factores normativos que afectan la eficacia de la Ley 29733 en diferentes segmentos empresariales financieros.
3. Determinar las consecuencias jurídicas y operativas del incumplimiento de la Ley 29733 en la protección de datos personales en el ámbito empresarial.

1.4. Justificación de la investigación

La protección de datos personales en la actualidad es un tema prioritario debido a los riesgos originados por el avance tecnológico y ciberataques, en especial en el sector financiero. La Ley 29733, Ley de Protección de Datos Personales en el Perú, tiene el objetivo de garantizar la protección de la información sensible, especialmente en empresas del sector financiero, ya que son los que manejan grandes números de datos personales. Pese a la normativa existente, su efectividad en la implementación práctica , sobre todo en los sistemas de ciberseguridad de las empresas financieras, sigue siendo un tema en disputa.

Luego, el sector financiero peruano se ve expuesto a progresivos riesgos de seguridad cibernética dado que maneja información sensible, lo que convierte aún más relevante el cumplimiento de la Ley de Protección de Datos Personales. Sin embargo, subsisten brechas normativas y operativas que limitan su eficacia en los distintos sectores empresariales. Esta situación puede desencadenar graves consecuencias jurídicas y operativas tanto para la empresa como para sus clientes, comprometiendo la información sensible y el derecho a la privacidad.

La presente investigación tiene el objetivo de analizar la eficacia de la Ley de Protección de Datos Personales dentro del marco de los sistemas de ciberseguridad empresarial financiero. Mediante un exhaustivo análisis de las brechas existentes, factores limitantes y las consecuencias que genera su incumplimiento, se busca ofrecer algunas propuestas para mejorar la implementación de esta norma, colaborando en un entorno más firme y confiable para el tratamiento de datos personales, con implicaciones significativas para las políticas empresariales y la defensa de los derechos de los ciudadanos.

1.5. Hipótesis

1.5.1. Hipótesis General

La eficacia de la Ley de Protección de Datos Personales en la implementación de sistemas de ciberseguridad empresarial está condicionada por el nivel de comprensión de sus parámetros normativos y la capacidad de adaptación a las necesidades específicas de cada empresa.

1.5.2. Hipótesis Específicas

a) Hipótesis Especifica 1

La limitada eficacia en la implementación de sistemas de ciberseguridad se debe principalmente a la falta de claridad en los parámetros técnico-normativos de la Ley de Protección de Datos Personales, así como a los altos costos de implementación, lo que dificulta su adopción por parte de empresas en crecimiento y compromete la seguridad de la información.

b) Hipótesis Especifica 2

La ausencia de criterios específicos en los artículos 16 y 17 de la Ley de Protección de Datos Personales (Ley 29733), que consideren el tamaño y la capacidad operativa de las empresas, junto con la insuficiente capacitación para su implementación, limita significativamente su eficacia en la protección de datos personales en los distintos segmentos empresariales. En ese contexto, la adopción de la norma ISO 27001 proporcionaría un marco estructurado y estandarizado para fortalecer la seguridad de la información, asegurando un cumplimiento más efectivo de la normativa y promoviendo una gestión integral de riesgos en la protección de datos en el país.

c) Hipótesis Específica 3

El incumplimiento de los parámetros para la protección de datos personales que establece la Ley 29733 exponen a la empresa a consecuencias jurídicas y operativas significativas. En el ámbito legal, la empresa puede enfrentar demandas civiles y responsabilidad penal en caso de delitos informáticos o filtraciones de información. Por otro lado, a nivel operativo, el incumplimiento

puede generar vulnerabilidades en los sistemas de seguridad, facilitando la exposición de datos sensibles de trabajadores y clientes, deteriorando la reputación de la empresa.

1.6. Marco Metodológico

El objeto de estudio de esta investigación es el análisis de la eficacia normativa de la Ley de Protección de Datos Personales en el sector empresarial financiero: Propuesta de mejora del marco jurídico para el fortalecimiento de la ciberseguridad corporativa.

Para este estudio, se adoptó un enfoque metodológico cualitativo de tipo descriptivo-exploratorio. Este enfoque, según lo define Hernández Sampieri, implica la recopilación de datos directamente relacionados con el objeto de estudio, con el propósito de perfeccionar las preguntas de investigación o identificar nuevas cuestiones durante el proceso de interpretación.[1]

Debido a la naturaleza del estudio, se optó por la metodología de investigación jurídico dogmático de tipo análisis crítico normativo. Esta metodología, según Reynaldo Tantaleán, se centra en el análisis del sistema normativo como la legislación y la doctrina. Este estudio es teórico y abstracto, pues permite a los investigadores cuestionar normas existentes y proponer nuevas soluciones, aunque su enfoque puede estar basado en el derecho puro, no ignora por completo la realidad social ya que las propuestas del investigador pueden influir en la creación y modificación de normas. Por tanto, la investigación jurídico dogmática analiza el derecho en un nivel abstracto, pero con el objetivo final de mejorar el ordenamiento jurídico y su impacto en la sociedad.[2]

Además, se empleó la técnica del análisis documental, que implica la búsqueda, selección, lectura, análisis e interpretación de datos provenientes de fuentes documentales relacionadas con el tema de estudio para responder a las preguntas y alcanzar los objetivos de la investigación. Por lo tanto, el presente estudio se clasifica como documental.

---

[1] Roberto Hernández Sampieri, Carlos Fernández Collado y María del Pilar Baptista Lucio, *Metodología de la Investigación,* 6a ed. (México: McGraw-Hill Education, 2014), 7.
[2] Reynaldo Mario Tantaleán Odar. *Tipología de las investigaciones jurídicas*. (Derecho y Cambio social, 2016), 4.

CAPÍTULO II: ANÁLISIS CRÍTICO

MARCO TEÓRICO

2.1. La Ley de Protección de Datos Personales en el Perú

2.1.1. Concepto y evolución de la Ley 29733

Desde hace una década, el Perú dispone de la Ley de Protección de Datos Personales, Ley N° 29733, cuyo propósito esencial es salvaguardar el derecho fundamental de los ciudadanos a la privacidad de su información personal. Para ello, establece normas para su tratamiento adecuado, asegurando que se realice con respeto a otros derechos fundamentales reconocidos en la legislación.[3]

En ese sentido, la Ley de Protección de Datos Personales (LPDP), "tiene como objetivo principal la regulación de los sistemas de almacenamiento, archivo, registro, sistematización y transmisión de datos personales, con la finalidad de proteger el derecho fundamental a la privacidad y la autodeterminación informativa que está contemplado en la Constitución"[4], específicamente en el artículo 2, inciso 6.

Esta ley tiene una naturaleza jurídica que puede considerarse como una ley de desarrollo constitucional, ya que establece normas que buscan garantizar la protección de datos personales en el marco de los derechos fundamentales de las personas.

Asimismo, los aspectos fundamentales que se destacan en la presente ley son; en primer lugar, los datos personales; según el numeral 2.4 de la LPDP, se define como toda información que se refiere a una persona natural, que permite su identificación o que puede hacerla identificable mediante medios que puedan ser razonablemente utilizados. El reglamento complementa esta definición, especificando que los datos personales pueden incluir información numérica,

[3] Superintendencia de Banca, Seguros y AFP (SBS) Informa. "Protección de datos personales: cautelando la seguridad de la información de los supervisados, usuarios y ciudadanos", Boletín Semanal N° 03, Febrero 2023, https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1250?title=Protecci%C3%B3n%20de%20datos%20personales:%20cautelando%20la%20seguridad%20de%20la%20informaci%C3%B3n%20de%20los%20supervisados,%20usuarios%20y%20ciudadanos#:~:text=Desde%20hace%2010%20a%C3%B1os%2C%20el,respeto%20de%20los%20dem%C3%A1s%20derechos

[4] Eguiguren Praeli, Francisco José. "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú." *THĒMIS-Revista de Derecho* 67 (2015): 131-140.

alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, entre otros[5]. En ese sentido, la amplitud de la definición de datos personales en la Ley de Protección de Datos Personales, es fundamental para garantizar una protección integral de la privacidad. Al incluir no sólo información identificadora directa, sino también aquella que podría hacer identificable a una persona mediante medios razonables, la norma busca evitar vacíos legales que puedan ser aprovechados para el uso indebido de datos. Además, la aclaración del reglamento sobre los diferentes tipos de datos personales (numéricos, alfabéticos, fotográficos, acústicos, etc.) es relevante, ya que reconoce la diversidad de información que puede comprometer la identidad o privacidad de un individuo. No obstante, el concepto de "medios razonablemente utilizados" puede ser sujeto de interpretación, lo que podría generar debates sobre su aplicación en casos concretos.

En segundo lugar; el banco de datos personales; de acuerdo con el numeral 2.1 de la LPDP, se entiende como un conjunto organizado de datos personales, automatizado o no, que puede estar almacenado en cualquier soporte, ya sea físico, magnético, digital, óptico u otros. Estos bancos de datos pueden ser gestionados tanto por personas naturales o jurídicas de derecho privado como por entidades públicas.[6] Asimismo, lo establecido por la LPDP permite abarcar distintos formatos y tecnologías de almacenamiento. Al no limitarse a sistemas automatizados o digitales, la norma reconoce que los datos personales pueden ser almacenados en soportes tradicionales, como archivos físicos, y en medios modernos, como bases de datos en la nube. Además, la inclusión de entidades públicas y privadas en la gestión de estos bancos refuerza la idea de que la protección de los datos personales debe aplicarse de manera generalizada, sin importar quién administre la información. Sin embargo, este enfoque también plantea desafíos en cuanto a la supervisión y cumplimiento de las normativas de seguridad, ya que la diversidad de responsables puede generar diferencias en la implementación de medidas de protección.

En tercer lugar; los datos sensibles; definido en el numeral 2.5 como aquellos datos personales compuestos por información biométrica que puede identificar al titular, así como datos relacionados con el origen racial o étnico, ingresos económicos, opiniones o creencias políticas,

[5] Eguiguren Praeli, Francisco José. "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú." *THĒMIS-Revista de Derecho* 67 (2015): 131-140.

[6] Ibid.

religiosas, filosóficas o morales, afiliación sindical, y cualquier información sobre salud o vida sexual. El reglamento, en su numeral 2.6, también aclara que los datos sensibles incluyen información sobre las características físicas, morales o emocionales de una persona, hechos o circunstancias relacionadas con su vida afectiva o familiar, hábitos personales que corresponden a su esfera más íntima, así como información sobre su salud física o mental u otros aspectos que puedan afectar su intimidad.[7] En esa línea de ideas, lo señalado por la LPDP es fundamental para garantizar la privacidad y evitar la discriminación basada en información altamente personal. La norma reconoce que estos datos, debido a su naturaleza, pueden ser utilizados de manera indebida para afectar los derechos fundamentales de las personas, como la igualdad, la no discriminación y la autodeterminación informativa.

En este sentido, se establece un nivel de protección más estricto para los datos sensibles, exigiendo medidas de seguridad reforzadas y restringiendo su tratamiento sin el consentimiento explícito del titular. Además, la regulación peruana se alinea con estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que también considera estas categorías de información como especialmente protegidas. Asimismo, el reglamento complementa esta definición al abarcar aspectos más subjetivos, como características emocionales y hábitos personales, lo que amplía la cobertura de protección. Sin embargo, esta amplitud también plantea desafíos en su aplicación, ya que algunas categorías, como "hechos o circunstancias de la vida afectiva o familiar", pueden ser difíciles de delimitar con precisión. Esto podría generar interpretaciones diversas y debates sobre los alcances de la protección, especialmente en contextos donde la recopilación de estos datos es necesaria para fines médicos, laborales o estadísticos.

No obstante, en la práctica, la aplicación de estas disposiciones enfrenta desafíos, especialmente en sectores como el de salud, empleo y políticas públicas, donde el tratamiento de datos sensibles puede ser necesario. Por ello, es crucial que tanto entidades públicas como privadas adopten mecanismos adecuados para el manejo seguro de estos datos, garantizando su uso legítimo sin vulnerar la privacidad de los ciudadanos.

---

[7] Eguiguren Praeli, Francisco José. "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú." *THĒMIS-Revista de Derecho* 67 (2015): 131-140.

Dicho esto, la Ley de Protección de Datos Personales en el Perú establece que su ámbito de aplicación se da a los datos personales almacenados en bancos de datos administrados por entidades públicas o privadas dentro del país, otorgando una protección especial a los datos sensibles. Sin embargo, existen excepciones a su aplicación. No se incluyen los datos almacenados para uso privado por personas naturales ni aquellos gestionados por entidades públicas cuando su tratamiento sea necesario para funciones específicas, como defensa nacional, seguridad pública o investigaciones penales.[8]

Aunque se reconoce la exclusión de datos utilizados con fines personales o familiares, se señala que la ley debería precisar si esto también aplica a registros empleados en actividades profesionales o laborales, como los de periodistas, abogados o médicos.

En términos generales, la LPDP abarca todos los archivos y bases de datos con fines económicos, administrativos, laborales o científicos, salvo las excepciones mencionadas. Su aplicación tiene un impacto significativo en la gestión de la información, promoviendo la seguridad, confidencialidad y protección de los derechos de los titulares de los datos.

2.1.2. ~~Principios~~ fundamentales de la Ley

Los principios fundamentales por los que se rige la Ley de Protección de Datos Personales en el Perú se encuentran regulados en los artículos 4 al 11, siendo ellos; i) el Principio de Legalidad, por cuanto señala que "el tratamiento de datos personales debe realizarse conforme a la ley. Se prohíbe además la recopilación de datos personales por medios fraudulentos, desleales o ilícitos."[9] ii) Principio de Consentimiento, este principio establece que es necesario el consentimiento previo, expreso e informado del titular para el uso de sus datos. iii) Principio de Finalidad; este principio resalta que los datos deben ser recopilados y usados únicamente para fines específicos, lícitos y previamente informados, "sin posibilidad de ser empleados para otros fines. Sin embargo, se permite su uso en investigaciones científicas, estadísticas o históricas, siempre que se apliquen procedimientos que garanticen la anonimización o disociación de la

---

[8] Eguiguren Praeli, Francisco José. "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú." *THĒMIS-Revista de Derecho* 67 (2015): 131-140.

[9] Ley 29733, de 3 de julio, Ley de Protección de Datos Personales. (Lima, 3 de julio de 2011)

identidad del titular."[10] iv) Principio de Proporcionalidad; este principio dispone que sólo deben recolectarse los datos necesarios para la finalidad establecida. v) Principio de Calidad; este principio establece que "los datos deben ser exactos, completos y actualizados. Además, resalta que estos datos deben conservarse de tal forma que se garantice su seguridad por el tiempo que requiera su tratamiento."[11] vi) Principio de Seguridad; este principio señala que se deben adoptar medidas para garantizar la protección de los datos personales contra accesos no autorizados o usos indebidos. vii) Principio de disposición de recursos administrativos y jurisdiccionales; este principio dispone que los titulares tienen derecho a reclamar y exigir la protección de sus datos. Por último, viii) Principio de Protección adecuada; este principio proscribe que se debe garantizar un nivel de protección adecuado en el tratamiento de los datos personales.

En ese sentido, se resalta que, estos principios buscan prevenir el uso indebido de los datos personales, asegurando su tratamiento dentro de un marco legal, con el consentimiento del titular y con medidas que garanticen su exactitud, seguridad y finalidad legítima. En conjunto, estas disposiciones refuerzan el derecho a la privacidad y la autodeterminación informativa, promoviendo un equilibrio entre el uso de la información y la protección de los derechos individuales.

2.2. Ciberseguridad en el entorno empresarial financiero

2.2.1. Concepto de Ciberseguridad

La ciberseguridad es un conjunto de operaciones, tecnologías y procedimientos diseñados para resguardar y proteger los sistemas informáticos, dispositivos, redes y datos de accesos no autorizados, el cual tiene como objetivo principal garantizar la integridad y privacidad de la información digital.

De ese modo, la ciberseguridad surge como una prioridad crucial por muchos motivos importantes que tienen un gran impacto a nivel personal como empresarial. La protección de información sensible se ha vuelto necesaria dentro de un entorno donde se acumula, almacena y

[10] Eguiguren Praeli, Francisco José. "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú." *THĒMIS-Revista de Derecho* 67 (2015): 131-140.

[11] Ley 29733, de 3 de julio, Ley de Protección de Datos Personales. (Lima, 3 de julio de 2011)

conserva una creciente cantidad de datos personales y financieros. Perder o no contar con un acceso autorizado a estos datos puede conllevar a graves consecuencias, desde el robo de identidad hasta el fraude financiero, perjudicando la seguridad y la confianza de las personas y las empresas.[12]

Dentro del sector empresarial, la continuidad de los negocios en su mayoría van a depender de la estabilidad y seguridad de los sistemas digitales. Un ciberataque logrado podría paralizar totalmente las operaciones de una empresa, lo cual desencadena pérdidas financieras significativas y daños reputacionales irreparables. Por lo tanto, la implementación de medidas efectivas de ciberseguridad se convierte en una necesidad imperiosa para garantizar la resiliencia y sostenibilidad de las organizaciones en un entorno digital altamente interconectado y vulnerable.[13]

Entonces, la ciberseguridad es fundamental para la protección de datos sensibles de los clientes dado que las datas de los mercados digitales almacenan una gran cantidad de datos, dentro de los cuales, además de contener su información personal, pueden incluir su historial de navegación, preferencias de compras, entre otras informaciones de índole privada. Exponer datos a ciberataques puede generar graves consecuencias como: robo financiero, fraude financiero, suplantación de identidad, etc.

Por otro lado, el propósito de la ciberseguridad es cumplir con algunos objetivos en la protección de activos digitales. Para una mejor comprensión acerca de la ciberseguridad y las protección de datos digitales, es importante considerar 3 conceptos significativos, los cuales son utilizados para guiar las políticas de seguridad de la información.

Sostener un sistema confiable y seguro consiste en asegurar los principios de confidencialidad, integridad y disponibilidad de los activos, entre otros elementos.[14]

---

[12] Aldrin Jefferson Calle García et al., "Importancia de la Ciberseguridad en la Investigación de Mercados Digital," *Ciencia y Desarrollo* 27, no. 2 (abril-junio 2024): 256-259.

[13] Ibid.

[14] José Manuel Ortega Candel, *Ciberseguridad: Manual Práctico*, 1ª ed. (Bogotá: Ecoe Ediciones, 2024), 3-9.

- *Confidencialidad:* Es un principio que señala que sólo los usuarios autorizados pueden tener acceso a los recursos de un sistema.
- *Integridad:* Es la propiedad de la información, la cual busca garantizar la precisión de los datos trasladados o almacenados, con lo cual podemos asegurar que no ha generado algún tipo de alteración, pérdida o destrucción, sea de manera accidental o intencionada. Esto también significa que los los recursos de un sistema sólo podrían ser utilizados y modificados por usuarios autorizados.
- *Disponibilidad*: Implica la capacidad de un servicio, una información o un sistema a ser accesible y utilizable por personal autorizado y cuando estos lo requieran. Estos recursos están a disposición de los usuarios autorizados.

En efecto, la ciberseguridad brinda protección de toda información que se preserva en el medio intangible del ciberespacio; sobre todo, datos sensibles concerniente a sistemas operativos. Los ataques ejecutados no solo son contra las instituciones financieras, sino también contra las instituciones gubernamentales, de transporte, industria, entre otros.[15]

2.2.2. Desafíos de la Ciberseguridad en el Sector Financiero

En la actualidad, las organizaciones públicas y privadas vienen enfrentando el reto de manejar grandes datas de información, debiendo estas ser administradas de forma segura, eficiente y eficaz. De esta manera, la cifra y tipo de información que poseen las organizaciones las transforma en el propósito de los ciberataques; eso significa que el nivel de riesgo existente es proporcional al nivel estratégico y técnico de la información que tiene a su amparo. Pese a ello, los ataques cibernéticos hacia los usuarios siguen en aumento. En general, los ataques cibernéticos los realizan contra bases de datos nacionales, sistemas financieros, entre otros.[16]

El sector financiero se ha convertido en uno de los principales objetivos para los ciberataques dado que este controla una gran cantidad de datos personales y financieros de sus clientes. Dentro

---

[15]Adolfo Arreola García, *Ciberseguridad: ¿Por qué es importante para todos?*, 1ª ed. (Ciudad de México: Siglo XXI Editores, Universidad Anáhuac, 2019)

[16] Ibid.

de este ámbito, la ciberseguridad es importante para garantizar la protección de datos personales, la confidencialidad de las transacciones y la confianza de sus clientes.

Los bancos, aseguradoras, empresas de inversión se enfrentan a grandes problemas como la gran dependencia de los sistemas tradicionales, riesgo cibernéticos y tecnológicos, cuestiones de cumplimiento normativo frente a la seguridad de información y aumento de competencia. Al modernizar los sistemas financieros a la nube, las organizaciones pueden mitigar estos desafíos y ofrecer mayores beneficios a los clientes.[17]

Los desafíos de la ciberseguridad en el sector empresarial financiero son diversos; entre los principales tenemos:

a) Ataques Cibernéticos:

- Phishing: Es un método que se fundamenta en la suplantación de identidad, en el cual los ciberdelincuentes envían correos electrónicos falsos que parecen legítimos y provenientes de empresas muy reconocidas. Dentro del mensaje adjuntan enlaces a sitios web fraudulentos o contienen archivos que buscan engañar al usuario para que proporcione información personal y financiera sensible. Los ciberdelincuentes, al obtener los números de cuentas bancarias, contraseñas o datos de tarjetas de crédito, pueden robar fondos, realizar transacciones no autorizadas o cometer cualquier otro tipo de fraude.
- Robo de identidad: Sucede cuando los delincuentes logran obtener y utilizar la información personal de los usuarios, tales como: nombres, dirección, datos bancarios, etc. para cometer algún fraude financiero a su nombre. A través de esta modalidad, los ciberdelincuentes pueden generar solicitudes de préstamos, aperturas de cuentas, etc.
- Malware: Es un software que se encarga de robar información confidencial, dañar dispositivos, realizar operaciones sin que el usuario se de cuenta. Esto se propaga mediante descargas aparentemente inofensivas, páginas web, enlaces en correos electrónicos, etc.
- Ransomware: Es un tipo de malware, el cual cifra los archivos y los datos de sistemas infectados, logrando bloquear el acceso a ellos hasta que paguen un tipo de rescate. Los

[17] Carolina César Piepenburg, "Desafíos de la Ciberseguridad en el Sector Financiero," *Intelequia*, 1 de agosto de 2024, https://intelequia.com/es/blog/post/desaf%C3%ADos-de-la-ciberseguridad-en-el-sector-financiero.

delincuentes lo utilizan con frecuencia para atacar a grandes organizaciones y exigirles altas sumas de dinero a cambio de entregarles la clave de descifrado. De no pagar el rescate, los archivos y datos podrían quedar inaccesibles permanentemente , causando pérdidas en las empresas y la interrupción de sus operaciones.

b) *Falta de recursos, conciencia y capacitación:*

Muchas organizaciones, en especial las PYMES, enfrentan una de las principales dificultades que es la falta de recursos financieros. La gran mayoría de estos negocios no tienen un presupuesto necesario para poder contratar a expertos en ciberseguridad o para aplicar tecnologías más avanzadas.

Por otro lado, muchos de los empleados de estas organizaciones no reciben una información adecuada en temas de ciberseguridad. La falta de capacitación y conciencia acerca de las amenazas cibernéticas y mejores prácticas puede conllevar a errores humanos, como hacer clic en enlaces maliciosos o hacer uso de contraseñas débiles. [18]

La ciberseguridad es un sector que demanda de la atención de profesionales cualificados, que tengan los conocimientos fundamentales y el liderazgo necesario para hacer frente a los problemas que van de la mano con los cambios tecnológicos constantes. Los vectores de amenazas avanzados y las nuevas tecnologías necesitan de profesionales de la ciberseguridad, con experiencia en tecnología, negocios y comunicación.[19]

2.3. Relación entre la Ley de Protección de Datos Personal y Ciberseguridad

Existe una familiaridad estrecha entre la Ley de Protección de Datos Personales y el concepto de Ciberseguridad, es así que la primera fue creada para asegurar la segunda en el extremo de

---

[18] Pepa Pizcueta, "Ciberseguridad para PYMES: Desafíos y oportunidades," *Next Educación*, 1 de octubre de 2024, https://www.nexteducacion.com/noticias/ciberseguridad-para-pymes-desafios-y-oportunidades/.

[19] José Manuel Ortega Candel, *Ciberseguridad: Manual Práctico*, 1ª ed. (Bogotá: Ecoe Ediciones, 2024), 3-9.

proteger aquellas toda información personal y sensible que pueda llegar a personas mal intencionadas, posibilidad cada vez mayor en esta era de las nuevas tecnologías.

La existencia de esta y otras normas que buscan proteger la Ciberseguridad de todos los ciudadanos es indispensable para garantizar la privacidad y seguridad de la información que se maneja en los contextos digitales. A continuación se mencionan la normativa específica para lograr una protección integral en materia de Ciberseguridad.

2.3.1. Normas específicas sobre protección de datos en sistemas de Ciberseguridad

Además de la Ley de Protección de Datos Personales, Ley N° 29733, nos encontramos con otra normativa necesaria o para el buen entendimiento y aplicación de esta norma o que sean de mayor especificidad para el control en ciertas áreas como la administración pública.

- Reglamento de la Ley de Protección de Datos Personales, Decreto Supremo N° 003-2013-JUS.

  Con este reglamento se busca la correcta aplicación de la LPDP, teniendo como mayores aportes la definición de los tipos de bancos de datos personales, la regulación de los niveles de seguridad en el manejo de datos personales, explicación de los derechos ARCO y establece medidas de seguridad informática para evitar ciberataques o mal tratamiento a las bases de datos personales[20].
- Directiva de Seguridad de la Información en la Administración Pública, DS N° 116-2017-PCM.

  Esta norma señala las directrices mandatorias para que las entidades estatales protejan su información digital. Las mayores contribuciones de esta Directiva ha sido la definición de roles y responsabilidades en la gestión de la seguridad de la información, la exigencia de medidas de ciberseguridad en el sector público, hacer obligatorio para las entidades públicas cumplir con el ISO 27001[21], entre otros.

---

[20] Perú, Reglamento de la Ley de Protección de Datos Personales, Decreto Supremo N.º 003-2013-JUS.

[21] Perú, Directiva de Seguridad de la Información en la Administración Pública, Decreto Supremo N.º 116-2017-PCM, El Peruano, 2017.

- Ley de Gobierno Digital, Ley N° 30999.

  Esta ley contribuyó con la creación del Sistema de Transformación Digital, promoviendo la interoperabilidad de sistemas estatales con seguridad digital y el establecimiento de las exigencia de estándares de protección de datos personales[22].
- Decreto Legislativo N.° 1412

  Este decreto regula el uso de tecnologías en el sector público. Como características, exige que los sistemas digitales del Estado cumplan con ciertas medidas de ciberseguridad, obliga la protección de los datos personales en plataformas del Estado y fomenta el uso de tecnologías seguras para la realización de trámites digitales[23].
- Ley de Delitos Informáticos, Ley N° 30096.

  También conocida como Ley de Ciberdelincuencia, esta ley penaliza los delitos informáticos y protege la privacidad digital. Ha tipificado diversos delitos, para así desincentivar a los posibles ciberdelincuentes en su accionar[24].

2.3.2. Incorporación de la Ley 29733 en políticas de seguridad empresarial

La ley 29733, Ley de Protección de Datos Personales, busca resguardar el derecho fundamental a la protección de los datos personales, que tiene correspondencia en el artículo 2 numeral 6 de nuestra Constitución Política del Perú.

La Ley de Protección de Datos Personales establece un marco legislativo que las empresas deben acatar para asegurar el tratamiento adecuado de la información sensible y personal[25], esto debe ser así por la importancia y valor económico que esta información tiene en el mercado.

Para ejemplificar esto, la ley tiene varios puntos que pueden ser cómodamente incorporados (y deben serlo) en las políticas de seguridad empresarial. Tenemos que debe existir un consentimiento explícito por parte del titular de los datos para que la empresa recopile y utilice su

---

[22] Perú, Ley de Gobierno Digital, Ley N.º 30999, El Peruano, 2019.
[23] Perú, Decreto Legislativo N.º 1412, Decreto de Gobierno Digital, El Peruano, 2018.
[24] Perú, Ley de Delitos Informáticos, Ley N.º 30096, El Peruano, 2013.

[25] Cámara de Comercio Americana del Perú (AmCham Perú), "Protección de datos personales: un imperativo legal y ético para las empresas en la era digital", AmCham Perú, acceso 22 de febrero de 2025, https://amcham.org.pe/news/proteccion-de-datos-personales-un-imperativo-legal-y-etico-para-las-empresas-en-la-era-digital/?form=MG0AV3.

información[26]. Además, en la ley existe de manera implícita un principio de transparencia que indica que las empresas u organizaciones deberán informar con claridad la finalidad de la recopilación de los datos, el uso que se les dará y las condiciones para su transferencia.

La norma exige que las empresas u organizaciones que manejen datos personales deberán inscribirse ante la Autoridad Nacional de Protección de Datos Personales, indicando aquí el tipo de datos que se maneja, los responsables de su tratamiento y las medidas de seguridad a implementarse. También exige la incorporación de medidas de seguridad (legales y técnicas) para el aseguramiento de la protección de estos datos.

Por último, consideramos que la incorporación de los Derechos ARCO (acceso, rectificación, cancelación y oposición) es un importante aporte que sirve para el aseguramiento de los derechos de las personas que se encuentran en este contexto.

Es fundamental la incorporación de la Ley 297333 en las políticas de seguridad empresarial para la reducción de riesgos legales y posibles sanciones. En adición a esto, ayuda al fortalecimiento de la ciberseguridad de la empresa al implementar medidas que prevengan los ciberataques, filtración de información y accesos sin autorización, protegiendo así a los clientes, empleados y la misma reputación de la empresa u organización.

[26] Ley N.° 29733 - Ley de Protección de Datos Personales (Perú): Publicada el 3 de julio de 2011 en el Diario Oficial El Peruano.

ANÁLISIS JURÍDICO

2.4. Alcance de la Ley N° 29733

La Ley N° 29733, conocida como la Ley de Protección de Datos Personales, tiene como objetivo regular el tratamiento de los datos personales en Perú, asegurando los derechos fundamentales de las personas relacionadas con su privacidad y protección de datos. La ley establece un marco normativo que deben seguir tanto las entidades públicas como privadas que manejen información personal. Su alcance es amplio y cubre el tratamiento de datos personales dentro del territorio peruano y en el contexto de servicios ofrecidos a personas en Perú, incluso si el responsable no se encuentra dentro del país.

Esta legislación se aplica a todas las entidades que recopilan y procesan datos personales, como empresas, organizaciones del gobierno, y otras entidades, sin importar su ubicación. Sin embargo, existen ciertas excepciones, como cuando los datos se recogen con fines personales o domésticos, o en investigaciones científicas o estadísticas, siempre que no afecten negativamente a los individuos involucrados. Además, la ley cubre datos sensibles, como información sobre salud, creencias religiosas o políticas, que requieren un tratamiento más riguroso.

Los responsables del tratamiento de datos personales tienen obligaciones claras bajo esta ley. Primero, deben obtener el consentimiento explícito e informado de los titulares de los datos antes de procesarlos, asegurándose de que las personas estén plenamente conscientes de qué datos se están recopilando y con qué propósito. Además, deben garantizar que los datos se traten solo para los fines específicos para los cuales fueron recolectados y que el procesamiento sea proporcional a esos fines, cumpliendo con el principio de minimización de datos.

La ley también exige que los responsables del tratamiento garanticen los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) de los titulares, lo que permite a las personas controlar su información personal. Además, deben implementar medidas de seguridad técnicas y organizativas para proteger los datos de accesos no autorizados y garantizar su integridad.

En caso de violaciones de seguridad que afecten los datos personales, la ley obliga a los responsables a notificar tanto a la autoridad nacional de protección de datos como a los titulares afectados para que puedan tomar medidas preventivas. También se requiere que los responsables mantengan un registro actualizado de las actividades de tratamiento y proporcionen acceso a la autoridad para verificar el cumplimiento de la ley.

Si los datos personales son transferidos a terceros, tanto dentro como fuera del país, se debe garantizar que se cumplan los principios establecidos por la ley y que el receptor de los datos ofrezca un nivel adecuado de protección. Cuando un responsable del tratamiento contrata a un tercero para procesar datos en su nombre, también debe asegurarse de que este cumpla con la ley y establecer acuerdos formales que regulen el tratamiento de los datos.

2.4.1. Ámbito de aplicación de la Ley de Datos Personales

La Ley N° 29733, Ley de Protección de Datos Personales, establece un marco legal para regular el manejo de datos personales en Perú, con el fin de proteger los derechos fundamentales relacionados con la privacidad y la seguridad de la información. Esta ley tiene un alcance amplio que incluye tanto a entidades públicas como privadas que realicen el tratamiento de datos personales.

La ley abarca a todas las organizaciones, ya sean públicas o privadas, que recopilen, procesen o utilicen datos personales, independientemente de si están ubicadas en Perú o en el extranjero, siempre y cuando realicen actividades relacionadas con ciudadanos peruanos o dentro del territorio nacional. Esto significa que, no solo las empresas locales deben cumplir con la ley, sino también aquellas extranjeras que manejen datos de personas peruanas.

En cuanto a las entidades públicas, la ley aplica a cualquier organismo del Estado que trate datos personales, como ministerios, autoridades gubernamentales o entidades encargadas de la administración pública. Estos organismos, como SUNAT o RENIEC, deben seguir los principios de la ley en la gestión de los datos que manejan.

Las entidades privadas también están sujetas a la ley si procesan datos personales. Esto incluye a empresas de diversos sectores, como los bancos, las compañías de telecomunicaciones, las

plataformas de comercio electrónico y servicios de salud. La ley busca que estas empresas respeten la privacidad de las personas y adopten medidas adecuadas para proteger los datos personales que gestionan[27].

El ámbito de aplicación de la ley también se extiende al tratamiento de datos dentro del país, sin importar si la entidad que los maneja está ubicada en Perú o fuera de él. Esto significa que si una empresa extranjera recolecta información personal de peruanos, también debe cumplir con las regulaciones de la ley.

No obstante, la ley no se aplica a situaciones donde los datos se usen exclusivamente para fines personales o domésticos, como en el caso de alguien que maneja información personal de familiares o amigos en un contexto privado.

Además, la ley establece reglas más estrictas para el tratamiento de datos sensibles, como aquellos relacionados con la salud, la orientación sexual o creencias religiosas. El consentimiento explícito de la persona es obligatorio para tratar estos datos, y su uso debe limitarse a lo estrictamente necesario y conforme a la ley[28].

En cuanto a las transferencias internacionales de datos, la ley establece que, si los datos personales se envían fuera de Perú, la entidad que los reciba en el país de destino debe garantizar la protección adecuada de los mismos. Esto significa que cualquier transferencia debe hacerse bajo estándares de seguridad que aseguren la confidencialidad y el respeto a los derechos de los individuos.

También, existen algunas excepciones, como en los casos en los que los datos se utilicen con fines académicos o científicos, siempre que no se afecten los derechos fundamentales de las personas involucradas. A pesar de estas excepciones, la ley exige que, incluso en estos casos, se mantengan los principios de protección de los datos personales.

---

[27] Fernando J. de la Vega, "Perspectivas sobre la protección de datos y la privacidad en la era digital," *Revista de Tecnología y Derecho* 7, no. 2 (2021): 20-21.

[28] María R. Córdova, "La privacidad y la protección de datos: Derechos y obligaciones en el Perú," *Anuario de Derecho* 14, no. 1 (2018): 30-31.

2.4.2. Deberes de los responsables del tratamiento de datos personales

La Ley N° 29733, conocida como la Ley de Protección de Datos Personales en Perú, establece varios deberes para quienes manejan datos personales con el fin de proteger la privacidad de los individuos y asegurar que la recolección y el tratamiento de los datos se realicen de manera legal y ética. Estos deberes son esenciales para garantizar el respeto de los derechos de los titulares de los datos.

En primer lugar, los responsables del tratamiento de datos deben permitir que las personas ejerzan sus derechos de acceso, rectificación, cancelación y oposición (conocidos como derechos ARCO)[29]. Esto implica que los individuos tienen el derecho de saber qué información se tiene sobre ellos, corregir errores, eliminar datos innecesarios o rechazar su tratamiento en circunstancias específicas.

Además, es obligatorio que los responsables obtengan el consentimiento previo, explícito e informado de los titulares antes de recolectar, almacenar o tratar sus datos personales. Este consentimiento debe ser claro y comprensible, asegurando que las personas entiendan cómo se utilizarán sus datos y por qué.

La ley también establece que los datos solo pueden ser recolectados con fines legítimos y específicos que deben ser claramente informados al titular al momento de la recolección. Los responsables no pueden usar los datos para otros fines diferentes a los que fueron inicialmente establecidos[30].

En cuanto a la recolección de datos, solo se deben obtener los datos necesarios para cumplir con la finalidad del tratamiento, y se debe evitar el almacenamiento de información excesiva o irrelevante. Además, los responsables deben tomar medidas adecuadas para proteger los datos personales, adoptando medidas técnicas, administrativas y organizativas que garanticen su seguridad y eviten el acceso no autorizado, la alteración o destrucción de los datos.

---

[29] César P. Salazar, *Derechos digitales y protección de datos en el Perú* (Lima: Editorial Jurídica Peruana, 2020), 102-103.

[30] Gonzalo M. Álvarez, "La protección de datos personales en el Perú: Análisis crítico de la Ley N° 29733," *Revista de Derecho Informático* 20, no. 1 (2019): 47-48.

La confidencialidad es otro aspecto clave, ya que los responsables deben asegurar que los datos personales no sean divulgados ni utilizados de manera inapropiada. Si ocurre un incidente de seguridad que afecte la integridad o confidencialidad de los datos, deben notificarlo tanto a la autoridad competente como, en algunos casos, a los titulares de los datos.

Si se requiere transferir datos personales a otros países, los responsables deben asegurarse de que el país receptor ofrezca un nivel adecuado de protección de datos, de modo que los derechos de los titulares no se vean comprometidos.

Asimismo, los responsables deben cumplir con todas las normativas relacionadas con la protección de datos personales y demostrar que están llevando a cabo sus responsabilidades de manera efectiva, implementando políticas y procedimientos adecuados para ello. También deben mantener un registro de las actividades de tratamiento de datos, que debe incluir detalles sobre el tipo de datos recolectados, las finalidades del tratamiento, los destinatarios y las medidas de seguridad implementadas. Este registro debe estar disponible para la autoridad de protección de datos cuando lo solicite.

2.5. Brechas entre el marco normativo y su implementación

2.5.1. Desafíos en la aplicación práctica de la Ley 29733

De acuerdo con la Autoridad Nacional de Protección de Datos, el nuevo reglamento de la Ley 29733 aprobado mediante “Decreto Supremo 016-2024-JUS tiene por finalidad asegurar la protección del derecho fundamental a la protección de datos personales, estableciendo normas para su manejo adecuado por parte de las personas naturales, entidades públicas y las instituciones pertenecientes al sector privado, especialmente en el ámbito digital”[31]; asimismo, tiene como novedad la introducción de la figura del oficial de datos dentro de las organizaciones que gestionen grandes volúmenes de información sensible. Además, el establecimiento de la obligación de notificar incidentes de seguridad. En consecuencia, las medidas contenidas en el

[31] Decreto Supremo N° 016-2024-JUS, de 30 de noviembre. Reglamento de la Ley 29733, Ley de Protección de Datos Personales. (Lima, 30 de noviembre de 2024)

reglamento tienen como objetivo el fortalecimiento de la gestión de datos, un aspecto que muchas empresas ya han incorporado en sus políticas de cumplimiento normativo (compliance) como parte de su proceso de digitalización acelerado durante la pandemia de COVID-19.

Asimismo, se establece que la figura del oficial de datos tiene la responsabilidad de supervisar el flujo de información dentro de la empresa. Para ello, es fundamental que cada organización realice una depuración de sus fuentes de datos con el fin de minimizar los riesgos. En esa línea de ideas, el reglamento enfatiza que los titulares de los datos serán responsables en caso de incidentes relacionados con sus proveedores, lo que obliga a las áreas de servicios y contratación a reforzar sus estándares de evaluación y revisar los protocolos de terceros.[32]

Por otro lado, se enfatiza que las organizaciones deberán adoptar un enfoque más integral en la gestión de incidentes, promoviendo una coordinación efectiva entre los departamentos de datos, relaciones públicas y legal para generar respuestas conjuntas. Actualmente, varias empresas multinacionales ya cumplen con estos requisitos como parte de sus programas de compliance alineados con estándares internacionales.[33]

Se debe destacar que, a nivel de dificultades en su implementación, el nuevo reglamento exigirá a las empresas realizar una mayor inversión para la incorporación de un oficial de datos y la adquisición de tecnología que permita identificar posibles fugas de información. En este contexto, sectores como el entretenimiento, servicios, retail y educación podrían enfrentar mayores dificultades en la gestión de datos, especialmente las pequeñas organizaciones, que a menudo carecen del presupuesto necesario para cumplir con estos requerimientos.[34]

Dicho esto, se evidencia un desafío clave en la implementación del nuevo reglamento: la inversión económica que las empresas deberán realizar para cumplir con las exigencias en materia de protección de datos; en tanto, la obligación de contratar un oficial de datos y adquirir tecnología especializada representa un reto significativo, sobre todo para sectores como

---

[32] Conexión Esan. Nuevos estándares para la protección de datos personales en el Perú. 04 de junio de 2024. https://www.esan.edu.pe/conexion-esan/nuevos-estandares-para-la-proteccion-de-datos-personales-en-el-peru

[33] Ibid.

[34] Ibid.

entretenimiento, servicios, retail y educación, donde la digitalización ha crecido rápidamente, pero sin necesariamente contar con estructuras sólidas de ciberseguridad.

Las pequeñas empresas enfrentan el mayor riesgo, ya que muchas de ellas operan con recursos limitados, lo que podría dificultar su capacidad para adaptarse a los nuevos estándares. Ante ello, se plantea la necesidad de que el Estado o la Autoridad Nacional de Protección de Datos ofrezcan incentivos, financiamiento o asistencia técnica para evitar que el cumplimiento de la normativa se convierta en una barrera que afecte su competitividad. En este sentido, sería beneficioso evaluar estrategias de implementación progresiva que permitan a las empresas adaptarse sin que su estabilidad financiera se vea comprometida.

Para mitigar este desafío, la Autoridad Nacional de Protección de Datos ha anunciado que las pequeñas empresas dispondrán de un plazo de hasta cuatro años para adecuarse a los nuevos estándares de protección de datos. Además, el reglamento considerará atenuantes de responsabilidad, como la implementación de políticas de protección de datos personales.[35]

En ese sentido, el plazo de cuatro años otorgado a las pequeñas empresas para adaptarse a los nuevos estándares de protección de datos es una medida que busca equilibrar la necesidad de cumplimiento normativo con la realidad financiera y operativa de estas organizaciones. Este tiempo adicional les permitirá ajustar sus procesos, capacitar a su personal y adquirir la tecnología necesaria sin que represente una carga económica inmediata.

Asimismo, la inclusión de atenuantes de responsabilidad, como la implementación de políticas de protección de datos personales, es una estrategia positiva, ya que incentiva a las empresas a adoptar buenas prácticas sin imponer sanciones desproporcionadas en caso de dificultades iniciales. Sin embargo, el éxito de esta medida dependerá de la asistencia técnica y el seguimiento que brinden las autoridades para garantizar una implementación efectiva y evitar que la flexibilidad se convierta en una excusa para postergar el cumplimiento de la normativa.

Ante este escenario, surge la interrogante sobre qué acciones debería tomar el Estado para garantizar que todas las empresas ajusten sus políticas conforme a la nueva normativa.

---

[35] Ibid.

2.5.2. Relación con otros marcos regulatorios internacionales

- **Unión Europea:**

El derecho a la protección de datos es un principio fundamental en la Unión Europea, consagrado en el Artículo 8 de la Carta de los Derechos Fundamentales. La regulación en esta materia se basa en el Reglamento General de Protección de Datos, la Directiva de Aplicación de la Ley y el Reglamento de Protección de Datos para Instituciones y Organismos de la UE, garantizando un marco normativo coherente a través de autoridades nacionales y europeas de supervisión.[36]

La implementación del Reglamento General de Protección de Datos, que entró en vigor en mayo de 2016 y se aplica desde mayo de 2018, marcando un hito en la protección de los derechos digitales y facilitó la actividad empresarial al armonizar normas y reducir cargas administrativas en el mercado único digital. Asimismo, su alcance se extiende al Espacio Económico Europeo.[37]

Por otro lado, los Estados miembros deben informar a la Comisión Europea sobre la implementación de sus disposiciones. En tanto, el Comité Europeo de Protección de Datos, el cual fue creado bajo el reglamento, es el organismo encargado de velar por la aplicación uniforme de las normativas de protección de datos en la Unión Europea y está compuesto por representantes de las autoridades nacionales de protección de datos, junto con el Supervisor Europeo de Protección de Datos, quien actúa como su secretaría. Sus funciones incluyen la emisión de orientaciones generales, la asesoría a la Comisión Europea sobre nuevas normativas y la resolución de disputas entre autoridades nacionales en materia de protección de datos.[38]

- **España:**

El marco regulatorio de protección de datos personales en España se basa en la normativa europea y nacional, con énfasis en el derecho al olvido y la responsabilidad de los motores de búsqueda en el tratamiento de datos personales.

---

[36] European Commission. Marco Jurídico de la protección de datos de la UE. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

[37] Ibid.

[38] Ibid.

El Tribunal de Justicia de la Unión Europea, en una sentencia clave, respaldó la postura de la Agencia Española de Protección de Datos (AEPD), estableciendo que los buscadores como Google son responsables del tratamiento de datos personales y deben cumplir con la normativa europea. Esto permite a las personas solicitar la eliminación de referencias que afecten su privacidad, salvo que exista un interés público legítimo en su difusión.[39]

Asimismo, la Directiva 95/46/CE y la legislación española aplican a las empresas que operan en el país, incluso si su sede principal está en otro lugar. La AEPD ha defendido activamente el derecho de los ciudadanos a solicitar la cancelación u oposición a la difusión de sus datos personales cuando estos sean inexactos, irrelevantes o lesivos.

En esa línea de ideas, el Tribunal de Justicia de la Unión Europea, establece que el derecho al olvido, no es absoluto, sino que se pondera con la libertad de expresión e información; en consecuencia, se aplica solo a informaciones sin relevancia pública y no obliga a modificar las fuentes originales, sino únicamente a limitar su visibilidad en los buscadores.

En conclusión, España sigue un enfoque riguroso en la protección de datos personales, alineado con los estándares de la Unión Europea, garantizando el equilibrio entre privacidad y acceso a la información.

- **Colombia:**

El marco jurídico colombiano en materia de protección de datos personales se basa en tres pilares fundamentales, estos son; el derecho a la intimidad, el Habeas Data y la regulación de datos personales. Asimismo, la Constitución Política de Colombia en su artículo 15 garantiza el derecho a la intimidad personal y familiar, así como el derecho al buen nombre, además de permitir a los ciudadanos conocer, actualizar y rectificar la información que sobre ellos se almacena en bases de datos públicas o privadas.[40]

---

[39] Agencia Española de Protección de Datos (AEPD), Nota informativa: El Tribunal de Justicia de la Unión Europea respalda las tesis de la AEPD en relación con los buscadores y el derecho al olvido en internet, 13 de mayo de 2014.

https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_otros_documentos_nota_AEPD.pdf

[40] Diego Miranda Guzmán. Los datos personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado): enfoque, ámbito de aplicación y contenido. Universidad Externado de Colombia. (Colombia,

Asimismo, el Hábeas Data es un mecanismo que otorga a los titulares de la información el derecho a acceder, modificar y corregir datos inexactos o erróneos, en ese sentido, la Corte Constitucional ha establecido que el derecho a la autodeterminación informativa se vulnera cuando la información personal almacenada no es clara, veraz, completa o actualizada. Asimismo, las bases de datos pueden ser públicas o privadas; por cuanto las públicas son gestionadas por el Estado para la prestación de servicios esenciales, mientras que las privadas son utilizadas por empresas con fines comerciales. Además, los datos personales se clasifican en públicos, semiprivados o privados, dependiendo de su nivel de acceso y protección.[41]

No obstante, el marco normativo que regulaba la protección de datos se dio con la Ley 1266 de 2008, que desarrolló el Habeas Data en el ámbito financiero, crediticio y comercial, estableciendo derechos y obligaciones para titulares, fuentes, operadores y usuarios de información. Esta ley fue modificada por la Ley 2157 de 2021, que introdujo cambios en el tratamiento de datos, incluyendo el derecho al olvido y nuevas disposiciones sobre la caducidad de la información crediticia.[42]

La transferencia internacional de datos es un aspecto clave dentro de la normativa, ya que requiere un análisis previo para garantizar que el país receptor cuente con un nivel adecuado de protección. La Corte Constitucional, a través de diversas sentencias, ha abordado la protección de datos en el entorno digital y su relación con los derechos fundamentales como la dignidad humana, el buen nombre y la privacidad.

En conclusión, el sistema colombiano de protección de datos busca equilibrar el uso de la información personal con la garantía de los derechos fundamentales, estableciendo un marco normativo que protege a los ciudadanos ante posibles abusos en el tratamiento de su información.

- **México:**

2023) https://telecomunicaciones.uexternado.edu.co/los-datos-personales-y-su-regulacion-en-colombia-datos-sensibles-datos-publicos-semiprivado-y-privado-enfoque-ambito-de-aplicacion-y-contenido/

[41] Ibid.

[42] Ibid.

En México, el derecho a la protección de datos personales es un derecho fundamental y este se encuentra reconocido en el apartado A del artículo 6 del texto constitucional, asimismo, este derecho no es independiente, sino que a menudo se encuentra vinculado con otros derechos como la intimidad, privacidad, honor y propia imagen. Aunque estos últimos no están explícitamente mencionados en la Constitución Política de los Estados Unidos Mexicanos, sí están protegidos mediante tratados internacionales suscritos por el país.[43]

No obstante, la garantía de este derecho se establece a través de dos leyes especializadas: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Protección de Datos Personales en Posesión de los Particulares, las cuales regulan el tratamiento y la seguridad de la información personal en distintos ámbito. Por su parte la Ley General de Protección de Datos Personales en Posesión de los Particulares, vigente desde el 6 de julio de 2010, busca garantizar un tratamiento de datos que sea legítimo, controlado e informado, protegiendo así la privacidad y el derecho a la autodeterminación informativa de los ciudadanos.[44]

Hasta 2016, España representaba el 13,2% de la inversión extranjera directa en México, con aproximadamente 5.800 empresas establecidas en el país, mientras que las compañías de la Unión Europea alcanzaron el 33,5% de la inversión total. Muchas de estas empresas están controladas o participadas en más del 50% por grupos europeos, lo que implica que deben cumplir con el Reglamento General de Protección de Datos (RGPD). Aunque la legislación mexicana aún no ha adoptado medidas específicas para armonizar su normativa con el RGPD, es crucial difundir su contenido para asegurar una correcta aplicación en concordancia con el sistema legal mexicano.[45]

---

[43] Mildred, Arteaga Franco. "Smart Contratcs: Perspectivas en la legislación mexicana actual y consideraciones para su aplicación". Infotec Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. (Ciudad de México, 2023) p. 66-67. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/616/1/Smart%20contracts%20perspectivas%20en%20la%20legislaci%C3%B3n%20mexicana%20actual%20y%20consideraciones%20para%20su%20aplicaci%C3%B3n.pdf

[44] Garrigues. ¿Cómo se regula la protección de datos en Latinoamérica y cómo influye el RGPD? (2018) https://www.garrigues.com/es_ES/noticia/regula-proteccion-datos-latinoamerica-influye-rgpd

[45] Ibid.

2.6. Factores normativos que limitan la eficacia de la Ley 29733

La Ley de Protección de Datos Personales en el Perú tiene como objetivo garantizar la protección de datos personales y/o sensibles de los ciudadanos, pero todavía existen varios factores normativos que limitan la eficacia de la ley. Entre los principales tenemos:

a) Ambigüedad en el alcance de las medidas de seguridad (artículo 16)

   El artículo 16 de la Ley de Protección de Datos Personales establece que los titulares de bancos de datos personales deben adoptar "las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado". [46] La limitación de este artículo es porque no especifica qué tipo de medidas deberían implementarse ni cuáles son los estándares mínimos de seguridad requeridos, permitiendo a las empresas adoptar criterios subjetivos para establecer el nivel de protección de datos, lo cual podría originar brechas de seguridad debido a prácticas insuficientes.

b) Falta de efectividad de la norma y recursos limitados

   Si bien la ley establece directrices claras, la escasez de recursos humanos y financieros dentro de la Autoridad Nacional de Protección de Datos Personales podría obstaculizar la supervisión y sanción de los infractores. En general, un marco regulatorio con recursos insuficientes es complicado para asegurar que las entidades financieras cumplan con las disposiciones legales.

c) Transformación de nuevas tecnologías

   En la actualidad, el panorama digital y las tecnología emergentes son muy relevantes para y cambiantes en todos los sectores económicos; sin embargo, la norma no siempre tiene adecuadas herramientas legales para enfrentar los desafíos que desarrollan las nuevas tecnologías, lo que limitaría su efectividad.

d) Dificultades Financieras

---

[46] Congreso de la República del Perú, *Ley 29733, Ley de Protección de Datos Personales*, art. 16, 2011.

Con los cambios normativos, se exigirá a las empresas una inversión mucho mayor para agregar a un oficial de datos y adquirir la tecnología necesaria para detectar posibles fugas de información. De esta manera, varios sectores económicos, sobre todo las organizaciones de menor tamaño, estarían más expuestos a sufrir inconvenientes en la gestión de su información por no contar con un suficiente presupuesto.[47]

e) Vacíos legales

En muchos casos, ciertos términos de la ley podrían ser interpretados de forma ambigua o general, causando incertidumbre para los encargados de proteger los datos como para los titulares de los datos personales, generando interpretaciones contradictorias en la implementación de la ley.

f) Desconocimiento y sensibilización

Muchas personas, trabajadores, clientes, empresas, organizaciones y entidades no cuentan con el mismo nivel de conocimiento sobre la ley y sus derechos. La falta de importancia sobre la protección de datos personales en la población, puede ser un obstáculo para la aplicación eficaz de la ley.

g) Insuficiente Cooperación Internacional

Debido a que la mayoría de flujos de datos personales son transnacionales, la Ley de Protección de Datos Personales podría percibir limitaciones por la falta de acuerdos internacionales o la aplicación de disposiciones legales internacionales a fin de asegurar la protección de datos a nivel global.

h) Insuficiente protección en el entorno digital

Aunque la ley cuenta con barreras para garantizar la protección de datos en las plataformas digitales, como redes sociales u otros servicios que brinda Internet,

---

[47] Conexión ESAN, "Nuevos estándares para la protección de datos personales en el Perú," *Conexión ESAN*, 4 de junio de 2024, https://www.esan.edu.pe/conexion-esan/nuevos-estandares-para-la-proteccion-de-datos-personales-en-el-peru.

continuamente los usuarios no tienen un control real acerca de cómo se gestiona y almacena sus datos.

i) Deficiencia de mecanismos claros y fiscalización

Si bien la norma contempla sanciones para las infracciones, el procedimiento para emplear estas sanciones suele no ser claras y ágiles, generando que las vulneraciones a la norma no sean resueltas de forma rápida o efectiva.

2.7. Consecuencias jurídicas de la infracción de la Ley N° 29733

2.7.1. Sanciones y medidas correctivas

El incumplimiento por parte de los bancos de datos de la Ley N° 29733, Ley de Protección de Datos Personales, traerá consigo sanciones y medidas correctivas importantes que repercutirán en las personas jurídica o naturales y entidades públicas que los representen, esto debido a que la ley busca tutelar el derecho fundamental a la protección de datos personales, derecho que es sumamente importante y frágil debido a que esta información sirve para la identificación de los sujetos. Por lo tanto, la Ley ha impuesto sanciones administrativas y medidas correctivas para lograr el cumplimiento de la finalidad de la norma.

- Sanciones Administrativas:
  Las sanciones administrativas contenidas en la normas se categorizan en tres niveles: leves, graves y muy graves.
    - “Las infracciones leves son sancionadas con una multa mínima desde cero como cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT)”. Esta infracción refiere a no informar de manera oportuna sobre el tratamiento de los datos personales o no inscribir el banco de datos personales en la Autoridad Nacional de Protección de Datos Personales (ANDP).
    - “Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades

impositivas tributarias (UIT)". La infracción grave sucede cuando el titular del banco de datos personales recopila datos sin el consentimiento expreso del titular de los datos personales, cuando no garantiza los derechos ARCO y cuando no se prestan las medidas de seguridad idóneas para la protección de los datos.

- "Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT)". Este nivel más gravoso de infracción se da cuando se transfieren los datos personales a terceros sin autorización del titular o mandato legal, cuando se tratan los datos de manera inadecuada sin cumplir con lo señalado en la ley y la comisión de actos de negligencia por parte del banco de datos.

- Medidas Correctivas:

  Las medidas correctivas que encontramos en la Ley son:

  - Suspensión y/o prohibición del tratamiento de los datos.
  - Eliminación de los datos tratados ilegalmente.

2.7.2. Responsabilidad penal y civil

El irrespeto por la Ley de Protección de Datos Personales, ley 297333, puede conllevar en consecuencias penales y civiles. Respecto a las consecuencias penales, la ley por sí misma no establece cuales son los tipos penales, pero de manera análoga podemos consultar otros textos normativos como la Ley de Delitos Informáticos, ley 30096, que sí establece varios tipos relacionados con la vulneración a la protección de los datos personales, por ejemplo, en caso de acceso indebido a bancos de datos personales (3 a 5 años de cárcel), suplantación de identidad (3 a 6 años de cárcel), venta o cesión ilegal de datos personales (4 a 6 años de cárcel) o la difusión no autorizada por el titular de datos personales sensibles (hasta 7 años de cárcel).

Por otro lado, la responsabilidad civil se representa primordialmente en los derechos de daños, cuando un banco o titular autorizado para la manipulación de los datos personales utiliza estos de manera negligente o fuera del mandato de la ley, y este tratamiento conlleva perjuicio para el

titular de los datos, entonces este última se encuentra en su derecho para demandar por daños y perjuicios, pudiendo haber existido un daños económico e incluso uno moral o psicológico.

Por lo antes mencionado, es importante que las empresas o instituciones tengan un buen manejo de los datos personales, incorporando medidas o políticas de seguridad y cumplimiento normativo.

2.8. Consecuencias operativas en la seguridad de datos personales

La Ley N° 29733, Ley de Protección de Datos Personales en Perú, establece un marco normativo que regula las consecuencias operativas relacionadas con la seguridad de los datos personales. Esta normativa establece una serie de principios y requisitos destinados a garantizar la seguridad de la información desde su recolección hasta su almacenamiento y tratamiento. El cumplimiento de estos lineamientos tiene un impacto significativo tanto para las organizaciones responsables del tratamiento de datos como para los derechos de los individuos cuyos datos se manejan.

Una de las principales implicaciones operativas de la ley en lo que respecta a la seguridad de los datos es la obligación de los responsables de implementar medidas adecuadas para garantizar su protección. Estas medidas deben ser tanto técnicas como organizativas y buscan evitar el acceso no autorizado, la alteración, el robo, la pérdida o la destrucción de los datos personales. Para ello, se requiere el uso de tecnologías de seguridad como cifrado, firewalls, sistemas de control de accesos y auditorías periódicas, entre otras.

El incumplimiento de la ley en términos de seguridad de los datos puede traer consigo consecuencias severas para las entidades responsables. En primer lugar, la Autoridad Nacional de Protección de Datos Personales (ANPDP) puede imponer sanciones administrativas a las organizaciones que no cumplan con los estándares de seguridad requeridos o que no implementen las medidas necesarias para proteger la información. Dichas sanciones pueden incluir multas económicas, cuya magnitud dependerá de la gravedad de la infracción cometida.

Además de las sanciones económicas, la ley contempla que las entidades pueden ser responsables de los daños que sufran los titulares de los datos a causa de una violación de seguridad. Si los

datos personales son accedidos de manera ilegal, alterados o utilizados indebidamente, los titulares pueden demandar por daños a su privacidad o por el uso inapropiado de su información personal. Esto podría derivar en litigios que afecten la reputación de la entidad y perjudique su relación con los clientes.

Otra de las consecuencias operativas de la ley es la obligación de las organizaciones de notificar tanto a los titulares de los datos como a la autoridad competente si ocurre un incidente de seguridad que ponga en riesgo la integridad o confidencialidad de los datos personales. Este tipo de incidentes debe ser reportado en un plazo máximo de 72 horas desde su detección. Las empresas deben tener protocolos establecidos para responder a incidentes de seguridad, detallando las acciones tomadas para mitigar el daño, como suspender el acceso a los datos comprometidos o implementar medidas correctivas.

Además, la ley obliga a las organizaciones a realizar auditorías periódicas de sus procesos de seguridad, con el fin de asegurar que están cumpliendo con las normativas de protección de datos. Estas auditorías incluyen la revisión de las políticas de seguridad internas, pruebas de vulnerabilidad y la evaluación del cumplimiento de las normas de privacidad.

El incumplimiento de las disposiciones de seguridad de la Ley N° 29733 puede tener consecuencias reputacionales para las entidades que manejan datos personales. En un entorno en el que la confianza es fundamental, una violación de seguridad puede afectar la imagen de la empresa, reducir la confianza de los clientes y socios comerciales y, como resultado, disminuir la demanda de sus servicios o productos.

2.8.1. Impacto de la empresas en el sector financiero

El efecto de las empresas en el sector financiero, en el marco de la Ley N° 29733 de Protección de Datos Personales, es considerable debido a las rigurosas normativas de seguridad y privacidad que deben cumplir[48]. En el sector financiero, donde se manejan datos muy sensibles, como información personal, cuentas bancarias y transacciones financieras, el cumplimiento de la ley es

---

[48] Raúl Vásquez, *Protección de Datos Personales: Un Enfoque desde la Legislación Peruana* (Lima: Editorial Universitaria, 2020)

esencial para garantizar la confianza de los clientes y el adecuado desarrollo de las actividades comerciales[49].

El sector financiero se ve afectado de varias maneras por la aplicación de esta ley. En primer lugar, las instituciones financieras deben destinar importantes recursos en infraestructura tecnológica y en personal especializado para asegurarse de cumplir con los requisitos de seguridad establecidos por la ley. Esto incluye la adopción de sistemas de cifrado, el establecimiento de protocolos de acceso seguro, auditorías regulares y la implementación de medidas para evitar el acceso no autorizado, el robo y la pérdida de datos. Si bien estas inversiones implican costos adicionales, son fundamentales para evitar sanciones económicas y daños a la reputación[50].

Otro aspecto relevante es que las entidades financieras deben tener procedimientos sólidos para manejar los incidentes de seguridad relacionados con los datos personales. Si ocurre una brecha de seguridad, las empresas deben informar a los clientes afectados y a la autoridad reguladora dentro de los plazos establecidos por la ley, lo que puede generar un impacto operacional considerable. Si no se cumplen con los plazos o no se toman las medidas correctivas necesarias, las entidades pueden enfrentarse a sanciones severas, como multas económicas.

En cuanto a la reputación, las entidades financieras que no cumplan con la Ley de Protección de Datos Personales pueden experimentar una pérdida de confianza por parte de sus clientes. Dado que en el sector financiero la confianza es un recurso vital, cualquier fallo en la seguridad puede tener efectos perjudiciales. Los clientes pueden decidir cambiar de institución financiera si sienten que sus datos no están siendo adecuadamente resguardados, lo que afecta la estabilidad y el crecimiento de la entidad. Esto puede también generar un efecto en cadena, afectando las relaciones con inversores, socios comerciales y otros actores clave.

---

[49] Jimena García, *Privacidad y Protección de Datos Personales: Retos y Oportunidades en Perú* (Cusco: Universidad Andina del Cusco, 2019)

[50] Fernando Montalvão, *Seguridad de la Información y Protección de Datos en el Perú: Una Guía Práctica para Empresas* (Lima: IEP, 2021)

El cumplimiento de la ley también influye en la competitividad de las empresas dentro del sector financiero. Aquellas que gestionan de forma adecuada los datos personales y demuestren un firme compromiso con la protección de la privacidad pueden utilizar este factor como un punto diferenciador en el mercado, atrayendo a clientes que valoran la seguridad de sus datos. Por otro lado, las empresas que no cumplan con estas regulaciones pueden quedar rezagadas frente a aquellas que ofrezcan mayores garantías de protección de datos.

Por último, las empresas del sector financiero deben estar preparadas para llevar a cabo auditorías periódicas y mantener registros exhaustivos sobre todos los procesos relacionados con la protección de datos personales, lo cual requiere una gestión eficiente y una supervisión interna adecuada. En conclusión, el impacto de la Ley N° 29733 en el sector financiero es significativo, ya que obliga a las instituciones a invertir en seguridad, a cumplir con regulaciones estrictas y a gestionar riesgos operativos y reputacionales relacionados con la protección de los datos personales.

2.8.2. Pérdida de confianza y reputación empresarial

La pérdida de confianza y la reputación empresarial en el marco de la Ley N° 29733 de Protección de Datos Personales es un aspecto clave, especialmente en industrias como la financiera, donde la protección de la información personal de los clientes es esencial. Si una empresa no adopta las medidas necesarias para cumplir con esta ley, las repercusiones no solo son legales y operativas, sino que también afectan gravemente la imagen y la reputación de la empresa.

Cuando una compañía no cumple con los requisitos de la Ley de Protección de Datos Personales, los clientes pierden la confianza en ella, lo que puede ocasionar una disminución en su base de usuarios o consumidores. En el contexto actual, donde los consumidores están cada vez más conscientes de los riesgos de seguridad relacionados con sus datos personales, es probable que prefieran trasladarse a empresas que demuestren un mayor compromiso con la protección de su privacidad. Esta pérdida de confianza no se limita solo a los clientes directos, sino que también afecta a socios comerciales, inversionistas y otras partes interesadas que confían en que la empresa maneje adecuadamente información sensible.

La reputación de la empresa, que es uno de sus activos más valiosos, puede sufrir un daño considerable si no se siguen los estándares de protección de datos establecidos por la ley. En un mundo cada vez más digitalizado, los incidentes relacionados con violaciones de datos y filtraciones de información personal se difunden rápidamente, y las empresas que no toman las precauciones necesarias pueden ser objeto de un intenso escrutinio público. Los medios de comunicación, las redes sociales y las plataformas de evaluación amplifican la noticia de cualquier brecha de seguridad, lo que puede resultar en una crisis de confianza. Esta pérdida de reputación no solo afecta la imagen pública de la empresa, sino que también puede llevar a un boicot por parte de los consumidores, disminuir la lealtad de los usuarios y reducir el valor de la marca.

La pérdida de confianza también puede extenderse a otros actores en el sector, como bancos, aseguradoras y otras entidades que también gestionan datos personales sensibles. Las instituciones financieras, por ejemplo, dependen de la confianza en su capacidad para proteger la información confidencial de sus clientes. Si una entidad se ve envuelta en un escándalo relacionado con la mala gestión de datos personales, podría perder la capacidad de formar nuevas alianzas comerciales o incluso ver limitadas sus operaciones en ciertos mercados.

El impacto de una violación en la seguridad de los datos personales no se limita solo al corto plazo. A largo plazo, la empresa podría enfrentar una disminución en sus ingresos y dificultades para atraer a nuevos clientes. Recuperar la confianza de los consumidores perdidos puede ser un proceso largo y costoso, que involucra inversiones en nuevas tecnologías de seguridad, campañas de marketing para restaurar la reputación, y la implementación de políticas de transparencia más estrictas.

No obstante, la Ley N° 29733 también establece un protocolo de actuación en caso de que ocurra una brecha de seguridad. Las empresas tienen la obligación de notificar tanto a los clientes afectados como a las autoridades competentes, lo que podría mitigar parcialmente el impacto de la pérdida de confianza. Sin embargo, la sola existencia de un incidente de seguridad puede afectar gravemente la imagen de la empresa. En este sentido, la manera en que la empresa maneje los incidentes de seguridad y actúe con transparencia puede ayudar a recuperar, en parte, la confianza de los clientes, siempre que se actúe con rapidez y de manera efectiva.

CASOS RELEVANTES

2.9. Casos relevantes sobre el incumplimiento de la Ley N° 29733

2.9.1 Caso Hackeo a Interbank

En octubre del 2024, varios usuarios de Interbank reportaron que tenían inconvenientes para ingresar al aplicativo bancario y también a su billetera digital Plin. Luego de varios reportes, la entidad financiera emitió un comunicado en donde confirmaba la filtración de datos personales de un grupo de clientes, lo cual fue hecho por un tercero sin autorización de la misma entidad.

Es así que la entidad financiera señaló que buscará darle la tranquilidad a los clientes de Interbank, garantizando la seguridad de sus depósitos y todos sus productos financieros, por lo que sí podrían seguir utilizando sus servicios con total normalidad.[51]

El hacker “kzoldyck” aseguró haber accedido a datos personales sensibles de clientes de Interbank, como nombres, teléfonos, emails, número de cuentas y cvv, que representan un alto riesgo para la privacidad y seguridad de los usuarios. Afortunadamente, la entidad bancaria comunicó que no se han visto comprometidos los fondos y productos financieros, pero el acceso a información personal y de contacto podría desencadenar intentos de estafa, phishing y robo de identidad. En el comunicado oficial, Interbank afirmó haber desplegado “medidas de seguridad adicionales” para mitigar los efectos del ataque, aunque los detalles sobre estas acciones específicas aún no se han difundido[52].

Dentro de su marco normativo, Interbank se comprometen a proteger los datos personales de sus clientes siguiendo los estándares de seguridad establecidas por las leyes peruanas, principalmente en:[53]

---

[51] Redacción Gestión, "Interbank: Fiscalía en Ciberdelincuencia inició diligencias sobre presunto hackeo," Gestión, 30 de octubre de 2024, https://gestion.pe/economia/interbank-hackeo-fiscalia-en-ciberdelincuencia-inicio-diligencias-sobre-presunto-hackeo-indecopi-datos-de-usuarios-noticia/.

[52] "Hackeo a Interbank alerta al sector bancario: ¿Estamos seguros?"

[53] Interbank, "Avisos Legales: Políticas de Privacidad," Interbank, consultado el 18 de febrero de 2025, https://interbank.pe/avisos-legales?tabs=politicas-de-privacidad.

- Ley N° 29733, Ley de Protección de Datos Personales
- Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley N° 2973
- Directiva de Seguridad de la Información, aprobada por la Resolución Directoral N° 019-2013-JUS/DGPDP.
- Directiva para el Tratamiento de datos personales mediante Sistemas de Videovigilancia, aprobada por la Resolución Directoral N° 02-2020-JUS/ DGTAIPD.

Por otro lado, también mencionan que dentro de su marco normativo interno han implementado medidas técnicas, legales y organizativas exigidas por la normativa para garantizar la seguridad y protección de la información que les proporcionan sus clientes; enfocados siempre en prevenir la pérdida, el mal uso, alteración, el acceso sin autorización y el robo de dicha información. Además, expresan cumplir estrictamente con el deber de confidencialidad en relación con los datos personales de sus clientes.[54]

Sin embargo, en el caso del hackeo a la entidad financiera Interbank, podemos interpretar que existe un incumplimiento del artículo 16 de la Ley de Protección de Datos Personales, dado que la filtración advierte una posible falta de medidas adecuadas para salvaguardar la información personal de sus clientes.

> *"Artículo 16.- Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.*
>
> *Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.*

---

[54] Interbank, "Avisos Legales: Políticas de Privacidad," *Interbank*, consultado el 18 de febrero de 2025, https://interbank.pe/avisos-legales?tabs=politicas-de-privacidad.

> *Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo."*[55]

La filtración de datos sensibles, los cuales incluían nombres completos, números de teléfonos, tarjetas, fechas de nacimientos, detalles de transacciones bancarias, etc., es un claro indicador de que las medidas de seguridad adoptadas por Interbank no fueron suficientes para salvaguardar los datos de todos sus clientes.[56]

Posterior a los hechos, entidades peruanas como Indecopi y la Autoridad Nacional de Protección de Datos Personales, iniciaron las investigaciones preliminares correspondientes para así determinar el grado de responsabilidad y las posibles sanciones en relación a la vulneración de los sistemas de seguridad de Interbank.[57]

Además, la especialista Dra. Yesenia Vásquez Valencia, considera que se debe fortalecer los equipos de profesionales dedicados a la ciberseguridad. Para ello, es necesario que las empresas inviertan en auditorías y en realizar análisis de vulneraciones de manera periódica. También, considera fundamental que sea exigible el cumplimiento de la aplicación de la certificación ISO 27001, una certificación que garantiza la seguridad en la gestión de la información. [58]

El presente caso, evidenciaría también la vulneración de la norma ISO 27001, la cual contiene un marco para la gestión de la seguridad de la información. La norma exige a las organizaciones a que implemente los controles adecuados para que se proteja la confidencialidad, integridad y disponibilidad de la información, incluyendo las medidas adecuadas contra ciberataques. Una brecha de seguridad como la que sufrió Interbank demuestra que algunos de los controles

---

[55] Congreso de la República del Perú, *Ley 29733, Ley de Protección de Datos Personales*, art. 16, 2011.

[56] Infobae. "Robo de datos en Interbank al descubierto: así operó el hacker para sustraer información de clientes del banco". *Infobae*, 11 de noviembre de 2024.

[57] El Comercio, "Hackeo al Interbank: Indecopi anuncia investigación preliminar contra el Interbank," *El Comercio*, 15 de noviembre de 2024, https://elcomercio.pe/lima/hackeo-al-interbank-indecopi-anuncia-investigacion-preliminar-contra-el-interbank-lima-ultimas-noticia/?ref=ecr#google_vignette.

[58] Montoya, "Hackeo a Interbank evidencia el rol imprescindible de los profesionales de Ciberseguridad - Noticias Trujillo".

sugeridos por el ISO 27001 podrían no haber sido implementados de forma efectiva o que existieron vulnerabilidades no mitigadas en su sistema.

Uno de los aspectos clave de la ISO 27001 es la constante evaluación de riesgos y la aplicación de medidas correctivas frente a posibles amenazas. Si el hackeo se debió a fallos en la detección de intrusiones, credenciales comprometidas o configuraciones erróneas, esto significaría deficiencias en la aplicación de controles específicos del Anexo A de la norma, como la gestión de accesos, la protección contra malware o la respuesta a incidentes de seguridad. Asimismo, la norma requiere auditorías periódicas que podrían haber identificado anticipadamente estas vulnerabilidades.

Además, la norma destaca la importancia de la capacitación y concienciación del personal en temas de ciberseguridad. Si el ataque compromete técnicas de ingeniería social o phishing, podría quedar en evidencia fallos en la implementación de programas de sensibilización o en el cumplimiento de políticas de seguridad interna. La falta de una cultura de seguridad fuerte o robusta dentro de las organizaciones puede hacer que incluso los mejores controles técnicos sean insuficientes para prevenir ataques exitosos.

Finalmente, este caso manifiesta la importancia de que las entidades financieras adopten protocolos de seguridad más rigurosos y actualizados, así como desarrollar planes de respuestas efectivas frente a incidentes de ciberseguridad, logrando cumplir con la legislación vigente y proteger la información de todos sus clientes. El hackeo a Interbank podría relacionarse con el incumplimiento o la ineficaz aplicación de la ISO 27001, la cual no es una norma de aplicación obligatoria en Perú.

La entidad deberá analizar si sus controles eran adecuados y si se realizaron auditorías conforme a la norma para detectar posibles brechas..A medida que avancen las investigaciones de las autoridades peruanas, las entidades financieras de nuestro país enfrentan la responsabilidad de evaluar sus sistemas, mejorar sus prácticas de seguridad y fortalecer su compromiso con la privacidad y la protección de sus clientes.[59]

[59] Montoya, "Hackeo a Interbank evidencia el rol imprescindible de los profesionales de Ciberseguridad - Noticias Trujillo".

2.9.2. Caso Banco de Crédito del Perú - BCP

A pesar de haberlo negado en reiteradas ocasiones, el Banco de Crédito del Perú (BCP) confirmó los rumores que corrían por mediados de el 2018, rumores que referían a la sustracción de los datos personales de los clientes de tal banco. Finalmente, en diciembre del 2019, el BCP emite un comunicado confirmando que habrían sufrido un ataque informático en el 2018, lo cual posibilitó a terceros la extracción de datos personales como cuentas, saldos y número de tarjetas[60].

Es así que el Ministerio de Justicia y Derechos Humanos (MINJUSDH), por medio de la Autoridad Nacional de Protección de Datos Personales (ANPD), luego de la confirmación por parte del Banco, inició un proceso sancionador en razón de la filtración, para así determinar qué responsabilidad tenía el banco respecto a este hecho[61].

Precisamente, entre los años 2017 y 2018 se reportaron numerosos casos de ciberataques en el Perú, cuyas cifras aumentaron en 11%, según un estudio de Accenture[62]. Cuestión crítica que trae preocupación a las autoridades y empresas privadas del sector de banca especialmente.

Medidas de seguridad:

El Banco de Crédito del Perú afirma que toma las siguientes medidas para proteger la Ciberseguridad:

- Seguridad en bancos de datos, los cuales se encuentran registrados ante la Autoridad Nacional de Protección de Datos Personales (ANPD).
- Utilización de datos biométricos para mejorar la seguridad en la autenticación.
- Uso de fuentes legítimas para garantizar la veracidad de los datos.
- Medidas de seguridad adecuadas en transferencias internacionales de datos a terceros autorizados.
- Adecuación estricta a la normativa en materia de protección de datos personales.

---

[60] Del Risco, “Ciberseguridad y datos personales: El caso del BCP,” Enfoque Derecho.

[61] LP Derecho, “Minjus inicia proceso sancionador contra el BCP por filtración de datos,” LP Derecho.

[62] Del Risco, “Ciberseguridad y datos personales: El caso del BCP,” Enfoque Derecho.

- Ofrece canales de comunicación para la notificación de cambios en sus disposiciones de ciberseguridad.
- Aseguramiento del ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición) vía presencial y telefónica.

Reputación y pérdida de confianza:

Este incidente sucedido en el 2018 ha traído consecuencias para el BCP respecto a sus grupos de interés. De manera automática, al enterarse de la filtración de los datos personales, los clientes comenzaron a retirar su dinero y cambiar sus claves de acceso. Muchos decidieron realizar el cambio a otros bancos debido a la incertidumbre y miedo de perder su dinero. Por otro lado, otros grupos de interés como accionistas e inversionistas vieron peligrar su capital debido a la pérdida de reputación y confianza respecto a la sociedad. Los colaboradores del banco vieron peligrar sus puestos de trabajo, debido a que toda afectación a la entidad repercute también en los sujetos que la conforman. Todo esto agravado por la multa impuesta

Notamos que con la filtración de los datos personales se infiere que el BCP no logró proteger adecuadamente la información de sus clientes, cosa que solo bajo interpretación (puesto que la norma no es clara en sus alcances) podemos entender como una violación o incumplimiento al deber de confidencialidad y seguridad previsto en el artículo 16 y 17 de la ley respectivamente. A pesar de que la norma refiere a medidas de seguridad y la prohibición del tratamiento de datos personales por aquellas que no lo cumplan, no queda claro si en casos como este en los que se han cumplido con medidas pertinentes pero aún así ha existido un ciber robo de información de manera inevitable, encaja en este artículo para la aplicación de una sanción.

La ambigüedad del artículo 16 y 17 genera una laguna legal que puede ser utilizado por las empresas para eximirse de algún tipo de responsabilidad administrativa, civil o penal, escudándose en narrativas que los benefician pero que dejan en indefensión a la parte más débil, que son en estos casos quienes comparten su información personal. Si bien la ley y su reglamento señala niveles de gravedad y cómo ha de aplicarse la norma, no establece con claridad qué nivel de eficacia deben garantizar ni cómo evaluar si una entidad actuó con la diligencia debida antes

de un ataque. Por tanto, para evitar inseguridad jurídica, es recomendable que estas normas señalen con claridad su finalidad y alcance.

Además, el caso de ciberataque de 2018 al banco BCP pone en evidencia la necesidad de implementar un marco de seguridad de la información, así como lo hace la norma ISO 27002, la cual consideramos debe ser implementada con obligatoriedad en la normativa actual de la Ley de Protección de Datos Personales.

El banco BCP debería haber contado con una mayor eficiencia de sus comunicaciones a sus empleados, junto con una revisión continua de estas políticas que le permitieran adaptarse a las amenazas que cada vez se renuevan debido al avance de las nuevas tecnologías. Esto dicho se encuentra señalado en el ISO 27002. También podemos hablar de la regulación de la Gestión de Incidentes de Seguridad que el ISO 27002 establece, es así que, si el banco BCP hubiera establecido procedimientos eficientes y claros para la detección, reporte y respuesta de incidentes de seguridad, se podría haber evitado o podido solucionar rápidamente la filtración de los datos, no produciéndose así la gran pérdida de confianza por parte de los clientes y daño a su intimidad. Por último, la norma ISO también nos señala un ámbito muy importante para la gestión de esta información sensible como son los datos personales, esta siendo acerca de la Organización de la Seguridad. Esto indicado nos subraya la importancia del compromiso gerencial para la anticipación de la ocurrencia de ciberataques, es necesario para este fin una dirección con directrices claras y decisiones firmes, mejorando también la coordinación con las distintas áreas de la compañía.

En conclusión, la aplicación de la norma ISO 27002 podría haber disminuido considerablemente los riesgos y consecuencias del ciberataque al banco BCP en el año 2018. El aporte de mejoramientos de los controles, junto con una cultura organizacional orientada a la seguridad de la información, habría reforzado la protección de los datos personales de los clientes y evitado la pérdida de confianza a la compañía.

2.9.3. Caso Ripley

El presente caso deriva de la Resolución Directoral N° 06-2023-JUS/DGTAIPD-DPDP, emitida por el Ministerio de Justicia y Derechos Humanos del Perú, el cual tuvo como objeto la

investigación y sanción a Banco Ripley Perú S.A. por infracciones a la Ley N° 29733, Ley de Protección de Datos Personales (LPDP) y su reglamento.

En ese sentido, con fecha 13 de mayo de 2019, una ciudadana presentó una denuncia a través de la Hoja de Trámite N° 033351-2019MSC, en la que acusó a Banco Ripley de haber tratado sus datos personales de manera irregular, en violación de la Ley de Protección de Datos Personales (LPDP) y su reglamento (Decreto Supremo N° 003-2013-JUS).[63]

Las inspecciones y recopilación de pruebas permitieron a la autoridad detectar dos infracciones principales cometidas por Banco Ripley:

1. Tratamiento indebido de datos personales sin medidas de seguridad adecuadas, al permitir la modificación de datos personales y la emisión de una tarjeta de crédito sin validar correctamente la identidad de la persona que solicitaba el cambio.
2. Incumplimiento de la obligación de confidencialidad, al permitir el acceso de terceros no autorizados a los datos personales de la denunciante.

Como resultado de estas irregularidades, la Direcciòn de Fiscalizaciòn e Instrucciòn emitió un Informe de Fiscalización en el que se recomendó iniciar un procedimiento administrativo sancionador contra Banco Ripley. Por ello, con fecha 30 de julio de 2020, mediante la Resolución Directoral N° 081-2020-JUS/DGTAIPD-DFI, se formalizó el inicio del procedimiento sancionador contra Banco Ripley, imputándole las siguientes infracciones:

1. Falta de medidas de seguridad en el tratamiento de datos personales
    - Artículo 39 del Reglamento de la LPDP, que exige que los bancos de datos implementen registros de seguridad adecuados para evitar accesos no autorizados.
    - La fiscalización reveló que Banco Ripley permitió la modificación de datos personales usando un DNI no vigente, lo que violó los estándares de seguridad exigidos.[64]

---

[63] Ministerio de Justicia y Derechos Humanos del Perú, *Resolución Directoral N.º 06-2023-JUS/DGTAIPD-DPDP* (Lima: Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, de 13 enero de 2023), 1.

[64] Ibid.

2. Incumplimiento de la obligación de confidencialidad
    - Artículo 17 de la LPDP, que impone el deber de preservar la confidencialidad de los datos personales.
    - Se verificó que Banco Ripley permitió que terceros no autorizados accedieran a los datos personales de la denunciante.

Por otro lado, Banco Ripley presentó su defensa en diversas ocasiones; por lo que con fecha 25 de noviembre de 2020 alegó que exigir la presentación del DNI físico era suficiente para la modificación de datos personales, sin necesidad de validar su vigencia. Asimismo, el 02 de diciembre de 2020: Argumentó que sus sistemas ya registraban las acciones relevantes en la modificación de datos, aunque no detallaban todos los cambios puntuales. Finalmente, con fecha 19 de julio de 2021: Informó que había implementado un nuevo procedimiento con validación biométrica para actualizar los datos de los clientes.

En esa línea de ideas, Banco Ripley también argumentó que había sido sancionado por el mismo hecho por INDECOPI, lo que violaría el principio del "Non bis in ídem" (no ser sancionado dos veces por el mismo hecho).

Sin embargo, la autoridad determinó que las sanciones de INDECOPI estaban basadas en la Ley de Protección y Defensa del Consumidor, que protege el derecho a recibir un servicio idóneo, mientras que la sanción del Ministerio de Justicia se basó en la Ley de Protección de Datos Personales, que protege el derecho a la autodeterminación informativa. Por lo tanto, se concluyó que no hubo doble sanción por el mismo fundamento jurídico. Por otro lado, se descartó la violación del principio de "Non bis in ídem", ya que la sanción del Ministerio de Justicia y la de INDECOPI tenían fundamentos jurídicos distintos.

Finalmente, se determinó que no corresponde imputar responsabilidad a Banco Ripley Perú S.A. por la infracción leve señalada en el literal a) del numeral 1 del artículo 132 del Reglamento de la Ley de Protección de Datos Personales. Esta infracción hace referencia al tratamiento de datos personales sin cumplir con las medidas de seguridad exigidas por la normativa, específicamente en relación con la implementación de medidas establecidas en el último párrafo del artículo 39 del Reglamento de la LPDP.

Asimismo, la Autoridad Nacional de Datos Personales impuso a Banco Ripley Perú S.A. una sanción económica equivalente a 1,74 Unidades Impositivas Tributarias (U.I.T.) por llevar a cabo el tratamiento de datos personales de la denunciante en los procedimientos denominados "Modificación de datos personales" y "Emboce (emisión) de tarjeta de crédito" sin haber implementado las medidas de seguridad requeridas. Esta falta constituye una infracción leve según lo dispuesto en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP, que sanciona el tratamiento de datos personales sin cumplir con las medidas de seguridad establecidas en la normativa.

Además, se sanciona a Banco Ripley Perú S.A. con una multa de 24,75 U.I.T. por haber incumplido la obligación de confidencialidad estipulada en el artículo 17 de la LPDP, al permitir que terceros no autorizados accedieran a los datos personales de la denunciante. Este hecho constituye una infracción grave, conforme a lo establecido en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP, que sanciona el incumplimiento de la obligación de confidencialidad establecida en la Ley N.º 29733.

En el presente caso se advierte la infracción del artículo 16 de la Ley de Protección de Datos Personales, este artículo establece las medidas de seguridad del tratamiento de datos personales y señala que el titular del banco de datos personales debe tomar medidas técnicas, organizativas y legales a fin de que se garantice su seguridad y se evite su alteración, pérdida, tratamiento o acceso no autorizado; en esa línea de ideas en este caso se cometió la infracción porque Banco Ripley no adoptó las medidas de seguridad necesarias para proteger los datos personales de sus clientes. La falta de verificación de identidad y la ausencia de registros adecuados en su sistema informático facilitaron el acceso indebido a la información personal de la denunciante, lo que vulneró su derecho a la protección de datos. Esto demuestra la "falta de cumplimiento por garantizar la seguridad de la información y evitar su alteración, pérdida, tratamiento o acceso no autorizado."[65]

Asimismo, la vulneración del artículo 17 de la Ley de Datos Personales el cual establece la confidencialidad de los datos personales, y señala que el titular del banco de datos personales, el

[65] María de Lourdes Zamudio Salinas, *Reflexiones sobre la observancia del derecho fundamental a la protección de datos personales en diversos actos regulados por el Código Civil*, Ius et Praxis, no. 55 (diciembre 2022): 82.

encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los datos y sus antecedentes, en ese sentido; el Banco Ripley permitió el acceso indebido a los datos personales de la denunciante a terceros no autorizados. Esto constituye una violación grave del principio de confidencialidad y del derecho a la protección de datos personales, lo que llevó a la imposición de una sanción económica significativa. De ahí que, "el principio de confidencialidad en el tratamiento de datos personales es fundamental para proteger la privacidad y seguridad de los individuos. Su aplicación no solo es un requisito legal, sino una garantía para evitar la exposición no autorizada de información sensible. Sin embargo, en la práctica, muchas empresas y particulares no implementan adecuadamente estas medidas, lo que puede derivar en filtraciones de datos o usos indebidos de la información. Es crucial que tanto los titulares de datos como las entidades responsables sean conscientes de la importancia de este principio y lo cumplan rigurosamente para evitar posibles vulneraciones y sanciones."[66]

Por tanto, las infracciones a los artículos 16 y 17 de la LPDP representan un riesgo significativo para la seguridad y confidencialidad de los datos personales. Mientras que la falta de medidas de seguridad adecuadas establecida en el artículo 16 fue considerada una infracción leve, la vulneración del deber de confidencialidad contenido en el artículo 17 fue calificada como una infracción grave debido a la exposición de datos personales a terceros no autorizados. En este caso, se han impuesto sanciones económicas a la entidad responsable.

2.9.4. Caso Google Spain

1. Antecedentes del Caso

El litigio que originó el caso conocido como "Caso Costeja" tuvo su inicio en el año 2009, cuando Mariano Costeja González, un ciudadano español, presentó una queja ante la Agencia Española de Protección de Datos (AEPD). La razón de su reclamo se centraba en que, al realizar una búsqueda de su nombre en Google, aparecían enlaces hacia una noticia publicada en 1998 por el periódico La Vanguardia, en la cual se mencionaba una subasta de propiedades asociada a una deuda que ya había sido resuelta años atrás. Costeja consideraba que esa información ya no

[66] Ibid.

tenía relevancia, y que afectaba directamente su derecho a la privacidad y a la buena reputación, dado que los enlaces seguían apareciendo en los resultados de búsqueda, aunque la deuda ya había sido saldada. Según su punto de vista, dicho contenido no solo era irrelevante, sino que continuaba perjudicando su imagen personal al estar disponible en línea a pesar del tiempo transcurrido.

La AEPD, tras examinar la solicitud presentada por Costeja, determinó que tanto Google Spain como Google Inc. eran responsables de la gestión de los datos personales de los usuarios, incluso cuando estos datos procedieran de otros sitios web. Con base en esto, la AEPD ordenó que Google eliminara los enlaces mencionados de sus resultados de búsqueda, ya que consideraba que el derecho a la privacidad de Costeja debía prevalecer por encima de los intereses comerciales de la empresa. Sin embargo, Google decidió apelar la decisión ante la Audiencia Nacional en España, lo que resultó en que el caso fuera remitido al Tribunal de Justicia de la Unión Europea (TJUE) para su resolución definitiva.

En 2014, el Tribunal de Justicia de la Unión Europea emitió una sentencia que marcó un precedente fundamental en lo que respecta a la protección de la privacidad en el entorno digital. En esta sentencia, el TJUE reconoció el derecho al olvido como un principio esencial para la protección de la privacidad, resolviendo que los motores de búsqueda, como Google, tienen responsabilidad sobre el tratamiento de los datos personales al indexar contenidos de terceros. Esto implica que los motores de búsqueda son considerados responsables del tratamiento de los datos y deben cumplir con las leyes de protección de datos. El tribunal afirmó que los motores de búsqueda, al organizar y difundir información a través de su actividad de indexación, deben garantizar que se protejan los derechos de las personas respecto a su información personal.

A raíz de esta sentencia, se determinó que el derecho de un individuo a la privacidad podría prevalecer sobre el interés público en el acceso a la información. Por lo tanto, los motores de búsqueda tendrían la obligación de eliminar o desindexar información personal cuando dicha información ya no fuera pertinente, estuviera desactualizada o afectara negativamente la privacidad de la persona en cuestión. Así, el motor de búsqueda asume el rol de "sujeto pasivo", siendo responsable de asegurarse de que los datos personales no permanezcan accesibles en los resultados de búsqueda cuando ya no sean relevantes o puedan causar daño. Por otro lado, el

individuo afectado, en este caso Costeja, se convierte en el "sujeto activo", teniendo el derecho a solicitar la eliminación de información personal que sea irrelevante o desactualizada, sin importar que esa información haya sido publicada legalmente en su origen.

El concepto de derecho al olvido, por lo tanto, se posicionó como una herramienta clave para la protección de los derechos fundamentales de las personas ante la exposición de su información personal en plataformas digitales como los motores de búsqueda. La sentencia del TJUE refuerza la idea de que los motores de búsqueda son responsables del tratamiento de los datos personales al indexar y organizar la información proveniente de sitios web de terceros. El derecho al olvido se fundamenta en la necesidad de proteger la privacidad de los individuos, permitiéndoles que, en determinadas circunstancias, puedan solicitar que se elimine la información personal que ya no sea relevante o que afecte su reputación, incluso si esa información fue publicada de forma legal en su origen.

Desde la perspectiva de la vulneración de datos personales, esta jurisprudencia subraya que los motores de búsqueda, al tratar la información de los usuarios, están expuestos a responsabilidades si gestionan datos personales que afectan negativamente a los derechos de privacidad de los individuos[67]. Según el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (2016/679), el derecho al olvido se aplica a todas las personas físicas y les otorga el derecho de solicitar la eliminación de sus datos personales cuando estos ya no sean pertinentes. El TJUE también destacó que, en ciertos casos, los derechos de privacidad de las personas deben prevalecer por encima de otros intereses, tales como la libertad de información o los intereses económicos de las plataformas de búsqueda.

La Sentencia del Tribunal de Justicia de la Unión Europea (TJUE)

El tribunal también se encargó de resolver varias cuestiones prejudiciales planteadas por la Audiencia Nacional. Entre estas preguntas se encontraba si Google debía ser considerado responsable del tratamiento de los datos según la Directiva 95/46/CE, si la AEPD podía ordenar la eliminación de enlaces sin dirigirse previamente a los propietarios de los sitios web, y si los

---

[67] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010), 73.

motores de búsqueda debían cumplir con los derechos de supresión de datos, incluso cuando la información estuviera publicada legalmente en la web original. En su sentencia, el TJUE concluyó que los motores de búsqueda, como Google, realizan un tratamiento de datos personales al recopilar, organizar y difundir información a través de la indexación de los contenidos. Asimismo, resolvió que el derecho al olvido debía prevalecer sobre el interés público en la accesibilidad de la información, salvo en casos en los que la información esté relacionada con una figura pública o posea un interés público evidente.

Este caso no solo marcó un hito en la protección de la privacidad en línea, sino que también introdujo el concepto de derecho al olvido para los ciudadanos europeos, quienes ahora pueden solicitar la eliminación de información personal irrelevante o desactualizada de los resultados de búsqueda, incluso si dicha información fue publicada de manera lícita en una página web. Sin embargo, el tribunal dejó claro que el derecho al olvido no es absoluto y puede ser limitado en casos en los que la información sea de relevancia pública o esté relacionada con una persona de interés público, como figuras políticas o celebridades.

Tras el fallo del TJUE, Google implementó un sistema para gestionar las solicitudes de eliminación de enlaces de sus resultados de búsqueda. En su informe de 2015, la empresa explicó que consideraría diversos criterios antes de proceder a desindexar un enlace, tales como la relevancia pública del contenido, el tipo de información y su relación con el interés público o privado, la fuente de la información (por ejemplo, un artículo de una hemeroteca digital), y la temporalidad de la información (si esta era antigua o ya no era relevante). Este enfoque permitió a Google equilibrar el derecho de los individuos a la privacidad con la necesidad de garantizar el acceso a la información de interés público.

El caso también influyó en la creación del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que se adoptó en 2016 y entró en vigor en 2018. Aunque el RGPD no fue fruto directo del caso Costeja, la sentencia del TJUE actuó como un importante catalizador para el desarrollo y fortalecimiento de las leyes sobre protección de datos en la Unión Europea. El RGPD otorgó mayores derechos a los individuos, proporcionando un marco más coherente y consistente para la protección de los datos personales en toda la Unión Europea, subrayando la importancia del derecho al olvido.

En relación con la Ley de Protección de Datos Personales de Perú, el caso de Google tiene una estrecha relación con los artículos 16 y 17 de dicha ley, que establecen derechos fundamentales para la protección de los datos personales de los ciudadanos. El artículo 16 establece el derecho de acceso a los datos personales, lo que implica que cualquier individuo tiene el derecho a consultar la información vinculada a su nombre en bases de datos, incluidas las que aparecen en los motores de búsqueda. El artículo 17, por su parte, regula el derecho de cancelación, permitiendo que las personas soliciten la eliminación de sus datos personales cuando estos ya no sean necesarios. En el contexto de Google, la negativa inicial a eliminar los enlaces solicitados por Costeja González resalta la responsabilidad de los motores de búsqueda de evaluar la relevancia de los datos personales y de cumplir con las solicitudes de eliminación cuando sea pertinente.

Este análisis demuestra cómo el derecho al olvido y la protección de los datos personales están vinculados tanto a la legislación europea como a la peruana, consolidando la idea de que los individuos deben tener el control sobre el uso y la difusión de su información personal, especialmente cuando esta ya no sea relevante o necesaria para sus circunstancias actuales. A medida que las leyes sobre protección de datos continúan evolucionando, tanto en Perú como en otras regiones, es de esperar que los derechos de los ciudadanos sobre sus datos personales se fortalezcan aún más en el entorno digital.

Vulneracion de datos personales

En el contexto de la vulneración de datos personales, el derecho al olvido se erige como una herramienta clave para proteger los derechos fundamentales de las personas afectadas por la exposición de su información personal en plataformas de motores de búsqueda. Este derecho fue fortalecido con la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) en 2014, en el caso Costeja, en el que se reconoció que Google y otros motores de búsqueda son responsables del tratamiento de datos personales cuando indexan y gestionan información accesible en internet[68].

---

[68] Paul M. Schwartz, "The Value of Personal Data," *Harvard Law Review* 88, no. 75 (1992): 887.

El derecho al olvido establece que los motores de búsqueda deben garantizar que los datos personales que gestionan se eliminen o desindexen cuando ya no sean pertinentes, actualizados o cuando su conservación afecte negativamente la privacidad de la persona[69]. En este sentido, el motor de búsqueda asume el rol de sujeto pasivo, siendo responsable de asegurar que la información personal no esté disponible en los resultados de búsqueda cuando esta ya no sea relevante o cause perjuicio a los derechos fundamentales de la persona afectada.

La persona cuya información es procesada y expuesta por los motores de búsqueda, en este caso, se convierte en el sujeto activo del derecho al olvido. Es decir, el individuo tiene el derecho a solicitar la eliminación de información personal desactualizada o irrelevante, sin importar que dicha información haya sido publicada de manera legal en su origen.

Desde la perspectiva de la vulneración de datos personales, esta jurisprudencia resalta que los motores de búsqueda, al realizar el tratamiento de datos a través de la indexación, están expuestos a posibles responsabilidades cuando gestionan información personal de personas que no desean que ciertos datos estén disponibles de manera pública y accesible.

Según el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (2016/679), este derecho se aplica a todas las personas físicas, y cualquier individuo cuya información personal sea identificable por medio de su nombre, apellidos u otros identificadores tiene derecho a solicitar la eliminación de datos personales que ya no sean pertinentes. Esto significa que la persona tiene la facultad de ejercer su derecho al olvido cuando los datos expuestos ya no sean relevantes para su situación actual.

En cuanto a la vulneración de los derechos fundamentales de la persona, el fallo del TJUE resalta la importancia de la protección de la privacidad sobre otros intereses, como la libertad de información o los intereses económicos del motor de búsqueda. Así, aunque los motores de búsqueda tienen un papel crucial en la accesibilidad de la información en línea, deben equilibrar sus intereses con la protección de la privacidad de los usuarios, garantizando que la información

---

[69] Ibid.

personal no permanezca disponible cuando su conservación ya no sea necesaria o cuando pueda perjudicar los derechos del individuo.

Este principio, que se encuentra en el Reglamento 2016/679 de la Unión Europea, coincide con el marco normativo de protección de datos de otros países, como Perú, donde la Ley de Protección de Datos Personales también establece los derechos de acceso, rectificación, cancelación y oposición (ARCO), permitiendo a las personas ejercer un control sobre sus datos personales[70].

Preguntas Prejudiciales y Fundamentos Jurídicos

El tribunal, al examinar el caso, se enfrentó a diversas cuestiones prejudiciales planteadas por la Audiencia Nacional, entre ellas si Google debía ser considerado responsable del tratamiento de los datos bajo la Directiva 95/46/CE, si la AEPD podía ordenar la eliminación de enlaces sin dirigirse primero a los propietarios de los sitios web, y si los motores de búsqueda debían cumplir con los derechos de supresión de datos, incluso cuando la información estuviera publicada legalmente en la web original.

El TJUE determinó que la actividad de los motores de búsqueda como Google se considera un tratamiento de datos personales, ya que estos realizan diversas operaciones sobre los datos, como su recopilación, organización, almacenamiento y difusión. El tribunal también resolvió que el derecho al olvido debía prevalecer sobre el interés público en la accesibilidad de la información, a menos que la información esté relacionada con una figura pública o tenga un interés público evidente[71].

El Impacto del Caso y la Evolución del Derecho al Olvido

Este caso marcó un hito en la protección de la privacidad en internet, pues el TJUE reconoció que el derecho a la privacidad y a la protección de datos personales prevalecía sobre los intereses comerciales de los motores de búsqueda. La sentencia también introdujo el concepto de derecho al olvido para los ciudadanos europeos, permitiendo que estos soliciten la eliminación de

---

[70] Daniel J. Solove, "Understanding Privacy," *Harvard University Press* (2008), 117.

[71] Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004): 101.

información personal que sea irrelevante o desactualizada, incluso si dicha información ha sido publicada de manera lícita en una web.

El derecho al olvido también está relacionado con la libertad de expresión e información, por lo que el tribunal subrayó que este derecho no debe ser absoluto. En casos en los que la información tenga relevancia pública o esté relacionada con una persona de interés público, como figuras públicas o políticos, el derecho al olvido podría verse limitado por el interés público en el acceso a esa información.

Medidas Adoptadas por Google

Tras la sentencia, Google implementó un sistema para gestionar las solicitudes de eliminación de enlaces de sus resultados de búsqueda. En su informe de 2015, Google explicó que consideraría los siguientes criterios antes de proceder con la desindexación:

1. **Relevancia pública** del contenido.
2. **Tipo de información** y su conexión con el interés público o privado.
3. **Fuente de la información**, como la hemeroteca de un periódico digital.
4. **Temporalidad** de la información, considerando si es antigua.

Este enfoque permite a Google realizar un equilibrio entre la protección de la privacidad y el derecho a la información, garantizando que los datos sensibles solo sean desindexados si no afectan al interés público.

La Influencia en el RGPD

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, adoptado en 2016 y en vigor desde 2018, se vio influenciado por este caso. Aunque el RGPD no surgió directamente del Caso Costeja, este sí fue un catalizador clave para el desarrollo y fortalecimiento de las leyes sobre protección de datos personales en la UE. El RGPD amplió los derechos de los individuos, proporcionando un marco más consistente y coherente para la protección de los datos personales en toda la Unión Europea, subrayando la importancia del derecho al olvido.

2. Medidas de seguridad con las que contaba Goolge para evitar lo ocurrido

Antes de que surgiera este conflicto, Google, en calidad de motor de búsqueda, contaba con ciertos procedimientos y medidas de seguridad para garantizar la protección de los datos personales de los usuarios, aunque estas no resultaron suficientes para evitar el incidente[72].

Google proporcionaba una política de privacidad que explicaba cómo se recopilaban, utilizaban y compartían los datos personales de los usuarios. Sin embargo, esta política no abordaba de manera explícita situaciones como la eliminación de enlaces de búsqueda que estuvieran relacionados con datos personales ya no relevantes. Además, la empresa utilizaba algoritmos automatizados para indexar información de millones de páginas web, organizando los resultados de búsqueda según su relevancia, pero sin un filtro para identificar si la información seguía siendo adecuada o pertinente. Esto provocaba que se mantuvieran datos obsoletos o irrelevantes en los resultados de búsqueda. Aunque Google contaba con un sistema para la remoción de contenido en casos de violaciones de derechos de autor, a través de la Ley Digital Millennium Copyright Act (DMCA) en EE. UU., no existían procedimientos claros o específicos para abordar los derechos de privacidad en relación con los resultados de búsqueda.

A pesar de estos esfuerzos, la falta de un mecanismo adecuado para tratar los derechos de privacidad individual, especialmente en el contexto de información que ya no era relevante, se evidenció en este caso.

3. Reputación y pérdida de confianza

El impacto de este caso en la reputación de Google fue considerable, no solo en Europa, sino a nivel mundial, ya que evidenció la falta de control sobre el manejo de los datos personales por parte de los motores de búsqueda[73]. Los usuarios comenzaron a cuestionar si Google y otras plataformas de búsqueda realmente respetaban los derechos fundamentales de privacidad de las personas. Como respuesta a la sentencia, Google adoptó medidas para implementar un sistema más riguroso en cuanto a la evaluación de las solicitudes de eliminación de enlaces, con el fin de

---

[72] Bennett Cypher, "The Right to Be Forgotten: The Role of Personal Data in the Digital Age," in *The Globalization of Privacy*, ed. Paul M. Schwartz and Daniel J. Solove (London: Routledge, 2018), 156.

[73] Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007), 12.

abordar de manera más eficaz las preocupaciones sobre la privacidad en el ámbito digital. Esto incluyó una revisión de las políticas de privacidad y el desarrollo de tecnologías para automatizar el proceso de eliminación de enlaces.

El impacto en la reputación de Google fue significativo, no solo en el ámbito europeo, sino globalmente, ya que el caso puso en evidencia la falta de control sobre el manejo de los datos personales que los motores de búsqueda pueden difundir sin un examen cuidadoso de su relevancia. Tras la negativa de Google a eliminar los enlaces solicitados por Costeja González, se planteó una seria cuestión sobre el respeto por la privacidad de los individuos en el mundo digital.

Los usuarios comenzaron a cuestionar si los motores de búsqueda, y las grandes plataformas tecnológicas en general, respetaban de manera adecuada los derechos fundamentales de las personas en términos de privacidad y protección de datos. Google, como líder en tecnología y motores de búsqueda, enfrentó una grave pérdida de confianza de los usuarios que esperaban que sus derechos de privacidad fueran protegidos.

A nivel de imagen pública, el caso también afectó la percepción de Google como una empresa responsable. El hecho de que una de las empresas más grandes del mundo de la tecnología se negara a cumplir con la solicitud de un ciudadano común generó un debate sobre la falta de rendición de cuentas de estas empresas frente a los derechos individuales de los usuarios.

4. Medidas adoptadas para evitar futuros ataques

En respuesta al fallo del Tribunal de Justicia de la Unión Europea (TJUE), Google adoptó una serie de medidas que reflejaban la necesidad de reforzar sus políticas de privacidad y proteger de manera más eficaz los derechos de los usuarios[74]:

[74] Jorge F. V. D. Santillán, *Derecho a la privacidad y protección de datos personales en el Perú* (2020).

- **Establecimiento formal del derecho al olvido**: Google implementó un procedimiento oficial que permitía a los usuarios solicitar la eliminación de enlaces a información personal obsoleta o irrelevante que apareciera en los resultados de búsqueda. Este procedimiento fue diseñado para permitir a los usuarios ejercer su derecho a la supresión de sus datos personales.
- **Mejoras en las políticas de privacidad**: En un esfuerzo por aclarar las formas en que los usuarios podían ejercer sus derechos sobre sus datos personales, Google mejoró su política de privacidad, haciendo hincapié en la protección de los datos personales y proporcionando una mayor claridad sobre cómo los usuarios podían solicitar la eliminación de información vinculada a ellos.
- **Evaluación de relevancia de la información**: Google comenzó a realizar una evaluación más rigurosa sobre la pertinencia de los datos que se mostraban en los resultados de búsqueda, teniendo en cuenta si la información seguía siendo relevante o útil para el público en general, o si, por el contrario, debería eliminarse.
- **Adopción de nuevas tecnologías de gestión de datos**: Google invirtió en el desarrollo de nuevas tecnologías para automatizar el proceso de eliminación de enlaces y mejorar la protección de la privacidad de los usuarios. Este esfuerzo también incluía la creación de sistemas más robustos para gestionar solicitudes de eliminación de datos personales, así como un sistema de auditoría para revisar el cumplimiento de las solicitudes.
- **Asesoría jurídica y seguimiento normativo**: En el ámbito legal, Google ajustó sus procedimientos internos de cumplimiento normativo para garantizar que sus operaciones estuvieran alineadas con las leyes de protección de datos, como la Directiva 95/46/CE y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que reemplazó la Directiva.

5. Análisis en relación con los artículos 16 y 17 de la Ley de Protección de Datos Personales de Perú

La Ley N° 29733 de Protección de Datos Personales de Perú, en particular los artículos 16 y 17, establece derechos fundamentales de los ciudadanos sobre la protección de sus datos personales.

- **Artículo 16:**

La relación de este artículo con el caso Costeja radica en que las entidades responsables del tratamiento de datos personales deben implementar medidas de seguridad adecuadas para garantizar la protección de la información, evitando su pérdida, acceso o tratamiento no autorizado. En este caso, Google, al ser responsable de gestionar datos personales en forma de enlaces asociados al nombre de una persona en los resultados de búsqueda, debe asegurarse de adoptar medidas técnicas, organizativas y legales para proteger esos datos. Además, el artículo prohíbe el tratamiento de datos en bancos de datos que no cumplan con los requisitos de seguridad establecidos, lo cual resalta la responsabilidad de Google de tomar las medidas necesarias para asegurar que los datos personales de los usuarios estén protegidos. Esto es especialmente relevante en el caso de Costeja, ya que la plataforma de Google no solo debía asegurar la protección de los datos, sino también garantizar que la información mostrada en sus resultados de búsqueda fuera relevante y apropiada, como lo dictó la corte al exigir la eliminación de los enlaces relacionados con su nombre. En este sentido, el artículo 16 refuerza la importancia de la seguridad en el tratamiento de datos personales, estableciendo que las personas tienen el derecho de controlar la información sobre ellos, lo cual se conecta directamente con el derecho al olvido y la obligación de eliminar los datos que ya no son pertinentes o adecuados, tal como ocurrió en el caso del Sr. Costeja.

- **Artículo 17:**

En este artículo se aborda la confidencialidad de los datos personales. Establece que todas las personas involucradas en el manejo de datos personales, como el titular del banco de datos, los encargados y cualquier otra parte que participe en su tratamiento, deben mantener la confidencialidad de dicha información, incluso una vez que termine la relación con el titular de los datos.

El caso de Google Spain resalta la importancia de mantener la confidencialidad y proteger la información personal de los usuarios. El Tribunal indicó que las plataformas de búsqueda deben asegurarse de que los datos personales no sean revelados de manera innecesaria ni utilizados de forma que puedan poner en riesgo la privacidad de los individuos. Esta obligación de confidencialidad coincide con la idea de que las empresas deben ser responsables en el manejo de

los datos personales, protegiendo la información del usuario y cumpliendo con los principios establecidos por la ley.

Además, que la obligación de confidencialidad puede ser levantada en situaciones específicas, como cuando el titular de los datos da su consentimiento explícito o cuando existe una orden judicial. El caso de Google también plantea dudas sobre los límites de esta confidencialidad, especialmente en casos en los que la divulgación de información pueda ser considerada necesaria o justificada, si se trata de un requisito legal o por razones de interés público, esto podría contradecir la obligación general de mantener la confidencialidad.

La sentencia relacionada con el Artículo 16 sobre la seguridad del tratamiento de datos personales sugiere la necesidad de que las empresas del sector financiero que manejen datos sensibles estén obligadas a obtener certificaciones internacionales como la ISO 27001. Esta medida garantizaría que adopten prácticas estructuradas en la gestión de la seguridad de la información, elevando la confianza del consumidor. Además, es esencial establecer controles mínimos de seguridad alineados con el Anexo A de dicha norma, lo cual facilitaría la implementación de medidas comprobadas para proteger la información sensible y mejorar la respuesta ante incidentes. Se plantea la creación de un régimen de auditorías regulares y sanciones para las empresas incumplidoras, lo que aseguraría el cumplimiento de las normativas de seguridad y incentivaría a las organizaciones a mantener altos estándares en la protección de datos personales. Este enfoque integral contribuiría a un entorno más seguro y confiable.

Este caso no se da acerca de un delito informático como tal, sino que se trata de un delito derivado de la afectación a la privacidad e intimidad.

El caso Google y el deber de confidencialidad

El caso de Google y el deber de confidencialidad trata sobre la protección de los datos personales. Google podría afecgtar la confidencialidad al divulgar información sin consentimiento, especialmente datos sensibles. El derecho al olvido permite que los individuos pidan la eliminación de su información personal de los resultados de búsqueda, reforzando así la protección de la privacidad y el control sobre los datos públicos. Las plataformas como Google

deben garantizar que los datos no se compartan sin permiso y cumplir con las leyes de protección de datos.

Respecto a las sanciones aplicadas podemos decir que se impusieron sanciones monetarias directas, ademas de que el TJUE establecio ciertos principios legales que afectaron la operación de los motores de búsqueda en relación con la protección de datos personales: Responsabilidad de los motores de búsqueda; Derecho al olvido (como derecho derivado de la privacidad e intimidad) donde Google debe ahora atender estas solicitudes; cumplimiento de normativas, es un procedente para que google y otros motores de busqueda ajusten sus practicas y políticas para alinearse con la legislacion de protección de datos personales y, de no cumplirse con estas obligaciones pueden estar sujetas a sanciones administrativas.

Sobre la evaluación de la eficacia de la ley en estos casos:

La Ley N.º 29733 establece un marco para proteger la seguridad y confidencialidad de los datos personales, exigiendo medidas de seguridad adecuadas y el tratamiento transparente de la información. También obliga a notificar afectaciones de seguridad a las autoridades y, en algunos casos, a los titulares de los datos. Las organizaciones deben contar con un responsable de seguridad para garantizar el cumplimiento. La efectividad de la ley depende de su correcta implementación y el compromiso de las entidades.

Relación entre ISO 27001 y las deficiencias detectadas en la ley

La ISO 27001 ofrece un marco para gestionar la seguridad de la información, complementando la Ley N.º 29733 al abordar problemas comunes en la protección de datos. Exige evaluar riesgos, establecer políticas de seguridad, restringir accesos no autorizados y capacitar al personal para evitar errores. También incluye un proceso de gestión de incidentes para responder rápidamente ante brechas y asegura el cumplimiento normativo.

La sentencia de la Gran Sala aborda la protección de datos personales y la necesidad de equilibrar la privacidad con el interés público. Resalta la importancia de que los gestores de motores de búsqueda asuman responsabilidades claras y establezcan procedimientos para manejar solicitudes de eliminación de datos. La implementación de un Sistema de Gestión de Seguridad de la

Información (SGSI) según ISO 27001 es crucial para facilitar la protección de datos, garantizar el cumplimiento normativo y promover la mejora continua en un entorno digital en evolución.

Certificación ISO 27001 en favor de lo sucedido

La certificación ISO 27001 podría haber evitado incidentes como los del caso Costeja al proporcionar un enfoque sistemático para la gestión de la seguridad de la información. Esto incluiría evaluaciones de riesgos, políticas claras para la protección de datos, concienciación del personal, controles de acceso y definición de responsabilidades. Además, fomentaría procesos para gestionar solicitudes de eliminación de datos y una cultura de mejora continua, lo que habría permitido a Google gestionar proactivamente la protección de datos y prevenir los problemas detectados en ese caso.

Comparación internacional

El caso Costeja y la implementación de la ISO 27001 son relevantes al comparar con el GDPR de la Unión Europea y la adopción de normas ISO en protección de datos. El GDPR exige a las organizaciones medidas de seguridad para proteger la privacidad, coincidiendo con los estándares de ISO 27001, que establece un sistema de gestión de seguridad de la información (SGSI) con controles para identificar riesgos, implementar medidas de protección y responder a incidentes. Ambas normativas requieren evaluaciones de riesgos, controles de acceso y auditorías periódicas.

En la Unión Europea, aunque el GDPR no menciona explícitamente la ISO 27001, esta norma es útil para cumplir con los requisitos de seguridad del GDPR. En otros países, como Brasil y México, también se utilizan normas ISO para fortalecer las leyes locales de protección de datos, alineándose con principios similares al GDPR.

México y Brasil han incorporado la ISO 27001 y otros estándares internacionales en sus marcos regulatorios para mejorar la protección de datos personales. En México, la Ley Federal de Protección de Datos Personales (LFPDPPP) exige que las empresas manejen adecuadamente los datos personales, y aunque no menciona específicamente la ISO 27001, esta norma ayuda a cumplir con los requisitos de seguridad establecidos por la ley, como la protección contra accesos no autorizados y la pérdida de datos. Por su parte, en Brasil, la Lei Geral de Proteção de Dados

(LGPD) requiere que las empresas implementen medidas de seguridad para proteger la información personal. Aunque la ISO 27001 no está mencionada explícitamente en la ley, su adopción permite a las organizaciones cumplir con los estándares de seguridad de la LGPD, mejorando la gestión de riesgos y la protección de datos. Ambos países utilizan la ISO 27001 como una herramienta para fortalecer el cumplimiento de sus leyes de protección de datos.

2.10. Nuevo Reglamento de la Ley N° 29733 - DS N°016-2024

El Nuevo Reglamento de la Ley N° 29733 - DS N°016-2024 estipula que se considera como incidente de seguridad cualquier vulneración que comprometa la protección de los datos personales, ya sea por su destrucción, pérdida, alteración ilícita, o por la comunicación o exposición no autorizada de los mismos.

"Ante un incidente de seguridad, se deben realizar las siguientes notificaciones:

1. A la Autoridad, dentro de las 48 horas siguientes al conocimiento del incidente.
2. Al titular de los datos personales afectado, dentro de las 48 horas siguientes al conocimiento de que el incidente puede vulnerar sus derechos.

Además, se exige la documentación detallada de cada incidente de seguridad, incluyendo los hechos acontecidos, los efectos producidos y las medidas correctivas implementadas."[75]

Asimismo, el nuevo reglamento permite al titular del banco de datos realizar una evaluación del impacto de sus tratamientos de datos, especialmente en ciertos casos. Esta evaluación puede basarse en estándares ISO.[76]

Por otro lado, se definen normativas particulares para distintos tipos de procesamiento de datos, incluyendo aquellos que involucran grandes volúmenes de información, afectan a un amplio

[75] Estudio Echecopar. "Nuevo Reglamento de la Ley de Protección de Datos Personales". Estudio Echecopar Asociado a Baker & MacKenzie International, 03 de diciembre de 2024, https://www.echecopar.com.pe/publicaciones-nuevo-reglamento-de-la-ley-de-proteccion-de-datos-personales.html

[76] Rodrigo, Elias & Medrano Abogados. "Alerta Privacidad y Protección de Datos - Diciembre 2024". Rodrigo, Elias & Medrano Abogados, 22 de febrero de 2025, https://www.estudiorodrigo.com/alerta-privacidad-y-proteccion-de-datos-diciembre-2024/

número de personas, contienen datos sensibles o pueden comprometer los derechos y libertades de los titulares. En esencia, el objetivo es fortalecer la protección de los datos personales, especialmente en casos donde exista un alto nivel de riesgo.[77]

Respecto al tratamiento de los datos personales, el nuevo reglamento regula el deber de informar, por parte de las entidades responsables del manejo de los datos personales, respecto a la creación de perfiles de los usuarios y a la fuente de donde se han recopilado los datos personales en caso no hayan sido entregadas directamente por el titular[78].

También se ha dado un nuevo tratamiento específico para aquellos datos personales que estén orientados a cumplir un fin publicitario. Aquí se debe informar al titular, cuando éste lo requiera, acerca de la fuente de recopilación. Además, señala que el consentimiento expreso para el uso publicitario de los datos personales, se dará en el primer contacto con el titular de los mismos[79]. Esto se encuentra presente en el artículo 26 del Decreto Supremo 016-2024-JUS.

2.11. Propuestas de adaptación normativa para mejorar la ciberseguridad

Luego de revisar algunos casos, se han planteado las siguientes propuestas de adaptación normativa para mejorar la ciberseguridad, dentro del marco de la Ley 29733.

1. Incorporar la obligatoriedad de la certificación ISO 27001 en el reglamento de la Ley 29733, especialmente para entidades del sector financiero.

Una de las principales implementaciones necesarias es la de definir claramente los estándares mínimos de ciberseguridad dentro de la norma que deben adoptar las instituciones para proteger los datos personales. El artículo 16 de la Ley 29733, señala que las entidades deben adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado[80]; sin embargo no especifica qué constituye dichas medidas.

---

[77] Ibid.
[78] Perú, Decreto Supremo N.º 016-2024-JUS, El Peruano, 2024, 22 de febrero de 2025, https://img.lpderecho.pe/wp-content/uploads/2024/11/Decreto-Supremo-016-2024-JUS-LPDerecho.pdf.
[79] Ibid.

[80] Congreso de la República del Perú, *Ley 29733, Ley de Protección de Datos Personales*, art. 16, 2011.

Luego, en el Reglamento de la Ley de Protección de Datos Personales Decreto Supremo, 003 - 2013-JUS, precisamente en su artìculo 32, detalla lo siguiente:

> *Artículo 32.- Confidencialidad y seguridad.*
>
> *Los operadores de comunicaciones o telecomunicaciones deberán velar por la confidencialidad, seguridad y uso adecuado de cualquier dato personal obtenido como consecuencia de su actividad y adoptarán las medidas técnicas, legales y organizativas, conforme a lo establecido en la Ley y el presente reglamento, sin perjuicio de las medidas establecidas en las normas del sector de comunicaciones y telecomunicaciones que no se opongan a lo establecido en la Ley y el presente reglamento.*[81]

En el artìculo descrito del presente reglamento tampoco menciona expresamente las medidas específicas que debarìan adoptar las empresas o instituciones, basándose en su tipo, tamaño, régimen, etc, siendo este tambièn un artìculo ambiguo.

Actualmente, el nuevo Reglamento de la Ley 29733, Decreto Supremo 016-2024, entre su artìculo 47, inciso 1 señala que:

> *Artìculo 47.1 El responsable del tratamiento de datos personales debe contar con un documento de seguridad el cual debe ser aprobado formalmente y contar con fecha cierta. El documento de seguridad debe estar actualizado y contener como mínimo los procedimientos de gestión de accesos, la gestión de privilegios y la verificación periódica de los privilegios asignados referentes a los sistemas de información, incluyendo, plataformas tecnológicas, aplicaciones móviles, motores de bases de datos, entre otros, empleados para realizar el tratamiento de datos personales. Puede tomar como referencia los requisitos y controles indicados en la NTP-ISO/IEC 27001 vigente o alguna mejor práctica o estándar ampliamente reconocido en su sector. En el caso de*

[81]Perú, Decreto Supremo N.º 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales, art. 32, *El Peruano*, 2013.

> *las entidades públicas aplican lo dispuesto en las normas de gobierno digital y seguridad digital vigentes.*

El artìculo señalado sólo expresa que las empresas pueden tomar como referencia los requisitos y controles indicados en el ISO 27001 o alguna mejor práctica reconocido en su sector, sin embargo, no obliga a la entidades a que adopten los estándares de la norma ISO 27001, lo cual consideramos importante que sea incorporado dentro del reglamento y no solamente sea mencionado.

La cada vez mayor digitalización del sector financiero ha aumentado la exposición a amenazas de ciberataques en el sector financiero, por lo que se hace necesaria la implementación de manera obligatoria de la ISO 27001 en la legislación de Protección de Datos Personales en el Perú. Estos estándares internacionales establecen un marco de gestión para una mayor seguridad de la información, permitiendo así para las entidades financieras identificar y mitigar riesgos de manera más eficaz. De esta forma se evitarían las filtraciones de datos personales y posibles pérdidas económicas y pérdida de reputación y confianza por parte de los clientes.

La certificación ISO 27001 significa un gran aporte para esta búsqueda de erradicación de contingencias, y ayudaría a su vez a la estandarización de la seguridad en las entidades y empresas que operan a nivel nacional. La implementación de esta norma permitiría establecer controles y protocolos rápidos de respuestas ante incidentes, reduciendo la probabilidad, reduciendo significativamente la probabilidad de ataques cibernéticos como son el phishing, ransomware y robo de credenciales.

Un aspecto fundamental es el aumento de la confianza entre clientes e inversores. Las organizaciones que obtienen certificaciones reflejan su compromiso con la seguridad de la información, destacándose en un mercado donde la protección de datos es cada vez más apreciada. Además, la norma fomenta una cultura de seguridad dentro de la empresa, implementando capacitaciones para el personal y reduciendo las vulnerabilidades derivadas de errores humanos. La adopción de la norma ISO 27001 también contribuye a mejorar la eficiencia operativa mediante un enfoque basado en riesgos y la aplicación del ciclo PDCA (Planificar-Hacer-Verificar-Actuar), asegurando una mejora continua en la gestión de la seguridad

de la información. Este enfoque posibilita a las instituciones ajustarse a nuevas amenazas y tecnologías, optimizando así el uso de sus recursos.

Finalmente, es fundamental la incorporación obligatoria de la certificación ISO 27001 en el nuevo reglamento, especialmente para entidades del sector financiero debido a que manipulan datos personales sensibles. Esta certificación proporciona una base sólida para que las organizaciones implementen un enfoque sistemático para la gestión de la seguridad de la información, lo que reduciría significativamente los riesgos de brechas de datos y ciberataques; además de mejorar la imagen de la marca y la confianza de los clientes, ya que demuestra que la organización está comprometida con la protección de la información.[82]

2. Otorgamiento de facultades a los motores de búsqueda para supervisar la gestión de datos personales en sus resultados de búsqueda - Integración del caso Costeja al artículo 37 del Decreto Supremo 016-2024, que aprueba el reglamento de la Ley 29733.

El artículo 37 inciso 1 numeral 2 del reglamento del Decreto Supremo 016-2024 señala que:

> *Artículo 37. Designación del Oficial de Datos Personales*
>
> *37.1 El titular del banco de datos personales o responsable y el encargado de tratamiento deben designar a un Oficial de Datos Personales cuando:*
>
> *2. El titular del banco de datos o responsable del tratamiento o el encargado de tratamiento realicen tratamientos de grandes volúmenes de datos personales, en cantidad o tipo de datos, o que pueda afectar a un gran número de personas o cuando se trate de datos sensibles o cuando se produzca un perjuicio evidente a otros derechos o libertades del titular del dato personal*[83].

Si bien el presente artìculo especifica que todas las entidades que manipulan una gran cantidad de datos personales y/o datos sensibles deben designar a un Oficial de Datos Personales, consideramos que en dicho artìculo tambièn se debería incluir a los motores de búsqueda (como

[82]GlobalSuite Solutions, "¿Qué es la norma ISO 27001 y para qué sirve?", *GlobalSuite Solutions*, acceso 22 de febrero de 2025, https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/.
[83] Decreto Supremo N.º 016-2024-JUS, Reglamento, art. 37, inc. 1, num. 2, El Peruano, 2024.

Google, Share, Microsoft Edge, Firefox, etc.), otorgándoles un rol de “policías” tal como ocurrió en el Caso Costeja (en el cual hubo un conflicto entre la vulneración de datos personales e interés público) con el fin de que, al igual que las entidades locales encargadas del tratamiento de datos, tambièn puedan supervisar y gestionar la información que se filtra en los resultados de búsqueda. Es decir, que estos últimos tienen un rol muy importante dado que deberán encargarse de actualizar y cotejar la información que se coloquen en sus plataformas para garantizar que la información publicada sea pertinente y actualizada.

En este marco, los motores de búsqueda deberán asumir la responsabilidad de asegurar que los datos personales en sus resultados no estén desactualizados, incorrectos o irrelevantes, y tomar las acciones necesarias para eliminar los enlaces que no cumplan con esos criterios. Asimismo, los motores de búsqueda deben garantizar la seguridad y confidencialidad de los datos personales que manejan, permitiendo que los usuarios puedan ejercer plenamente sus derechos, incluido el derecho al olvido, de manera clara y eficiente.

En torno al sector financiero, un motor de búsqueda podrìa detectar o toma conocimiento acerca de la filtraciòn de datos sensibles de clientes de alguna entidad bancaria, por lo que inmediatamente tendrìa la responsabilidad de eliminar, suprimir y notificar sobre la información filtrada detectada para que la entidad y las autoridades pertinente tomen conocimiento, investiguen y tomen medidas necesarias para evitar un riesgo mayor.

Entonces, el papel que cumplirìan los motores de búsqueda serìan imprescindibles para garantizar la protección de datos personales y datos sensibles, sobre todo en sectores empresariales que manejan o manipulan grandes cantidades de información.

Las entidades financieras, mediante sus Oficiales de Protección, en colaboración con los motores de búsqueda, podrían supervisar la implementación de políticas adecuadas de protección de datos, asegurando que el tratamiento y eliminación de datos se ajuste a las regulaciones.

Siguiendo la jurisprudencia del caso Costeja, Google debe colaborar con las autoridades de protección de datos para garantizar que las solicitudes de eliminación de enlaces se gestionen de manera adecuada, protegiendo la privacidad de los usuarios y cumpliendo con las leyes locales.

2.12. Evaluación de la necesidad de reformas en la Ley N° 29733

La revisión de la Ley N° 29733 revela que, aunque representa un avance significativo, carece de la profundidad y rigor necesarios para abordar las amenazas cibernéticas actuales[84]. Esto ha sido evidenciado por incidentes como los ataques a Interbank, BCP, Ripley y Google Spain, los cuales han puesto en manifiesto las debilidades en el sistema de protección de datos[85].

Una alternativa para mejorar esta situación sería hacer que la norma ISO 27001 sea un requisito obligatorio dentro del reglamento de la ley, ya que se trata de un estándar internacionalmente reconocido que establece las mejores prácticas en ciberseguridad. Implementar esta norma podría potenciar de manera considerable la protección de los datos personales en el ámbito empresarial financiero. La ISO 27001 detalla la organización de un sistema de gestión de seguridad de la información (SGSI), abarcando aspectos cruciales como la evaluación de riesgos y la salvaguarda de la confidencialidad, integridad y disponibilidad de los datos.

La ISO 27001:2022 es una norma internacionalmente reconocida que establece un marco para la gestión de la seguridad de la información mediante la creación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema ayuda a las organizaciones a identificar, evaluar y mitigar riesgos asociados con la seguridad de los datos, asegurando la confidencialidad, integridad y disponibilidad de la información. Para el sector financiero en Perú, donde se procesan diariamente miles de transacciones y se almacena información personal de millones de clientes, contar con un SGSI basado en la ISO 27001 no solo es una ventaja competitiva, sino una necesidad operativa y regulatoria.[86]

En el sector financiero, que maneja grandes volúmenes de información sensible, adoptar un sistema como el de la ISO 27001 aseguraría una protección constante y estructurada ante los riesgos de ciberseguridad. Además, esta norma proporciona un marco integral para gestionar

---

[84] Ley N° 29733, Ley de protección de datos personales (Congreso de la República del Perú, 2011).
[85] Ministerio del Interior del Perú, *Informe sobre Incident Report in Cybersecurity*, 2023.
[86] NQA, I*SO 27001: 2022 Guía de Implementación de Sistemas de Gestión de Seguridad de la Información* (Reino Unido: NQA, 2022), 4-31.

dichos riesgos, lo que complementaría los esfuerzos de la Ley 29733 al ofrecer un enfoque más riguroso y profesional en la protección de datos personales.

Además de la protección contra ataques cibernéticos, la ISO 27001 garantiza el cumplimiento de regulaciones locales e internacionales. En Perú, la Ley de Protección de Datos Personales exige a las empresas implementar medidas adecuadas para salvaguardar la información de sus clientes. La certificación en ISO 27001 no solo ayudaría a las entidades financieras a cumplir con estos requisitos, sino que también facilitaría su integración en mercados internacionales donde esta norma es un estándar de referencia.[87]

Otro aspecto importante es la confianza del cliente y la reputación corporativa. En un contexto donde la seguridad de la información es una preocupación que va en aumento, las instituciones financieras deben demostrar su compromiso con la protección de los datos. Contar con la certificación en ISO 27001 les permitiría a las organizaciones diferenciarse de la competencia y asegurar a sus clientes que sus informaciones están siendo manejadas bajo los más altos estándares de seguridad.

Al incorporar la ISO 27001 en el reglamento, las entidades del sector financiero no solo estarían mejor preparadas frente a incidentes de seguridad, sino que también demostrarían su compromiso con la mejora continua en la gestión de la seguridad de la información.

Entre los beneficios de implementar esta norma se incluyen:

- **Mayor confianza:** Los clientes y usuarios tendrían más tranquilidad al saber que las entidades financieras están alineadas con estándares internacionales de seguridad para proteger sus datos personales.

- **Reducción de riesgos:** La norma facilita la identificación y gestión eficaz de los riesgos, lo que reduce las posibilidades de sufrir ciberataques o violaciones de seguridad.

[87] Ibid.

- **Cumplimiento normativo:** Garantiza que las entidades financieras no solo respeten la Ley 29733, sino que también se adhieran a un marco global de buenas prácticas en ciberseguridad.

La inclusión de esta certificación en el reglamento de la ley proporcionaría una base más robusta y coherente para fortalecer las políticas de ciberseguridad en el sector financiero, asegurando así una mayor protección de los datos personales de los usuarios[88].

Siguiendo como ejemplo, paìses como Reino Unido, Australia y Alemania, se han adoptada a los normas ISO 27001:

- **Reino Unido**: En el Reino Unido, la implementación de la ISO 27001 ha sido ampliamente adoptada, especialmente en el sector bancario y de servicios financieros, debido a las estrictas regulaciones de seguridad de la información. Además, el Reino Unido tiene un marco regulador que alienta a las empresas a adoptar normas internacionales como la ISO 27001 para cumplir con los requisitos de protección de datos.[89]

  Australia: En Australia, la ISO 27001 es utilizada en varias industrias, incluidas las financieras y gubernamentales, para cumplir con los requisitos de la Ley de Privacidad. El gobierno australiano ha promovido la adopción de estándares internacionales de seguridad cibernética para proteger los datos sensibles, especialmente después de varios incidentes cibernéticos que afectaron tanto a empresas privadas como a entidades públicas.[90]

  Alemania: Alemania ha sido pionera en la adopción de la **ISO 27001**, especialmente en sus sectores financieros y de tecnología. Las regulaciones como la **Ley de Protección de Datos** y las directrices del **Comité Federal de Seguridad de la Información (BSI)** han

[88] "Estudio sobre la implementación de la norma ISO 27001 en el sector financiero," *Revista de Seguridad de la Información,* 2023

[89] UK Government. (2021). *Cyber Security: Protecting your Organisation*. Retrieved from https://www.gov.uk/guidance/cyber-security.

[90] Australian Government. (2020). *Cyber Security Strategy 2020*. Retrieved from https://www.cyber.gov.au.

impulsado la adopción de esta norma para cumplir con los estándares de protección de datos y ciberseguridad.[91]

La obligatoriedad de la ISO 27001 en el sector financiero en Perú es una medida estratégica para fortalecer la ciberseguridad y garantizar la protección de los datos. Con la creciente digitalización de los servicios financieros, es imperativo que las organizaciones adopten esta norma para reducir riesgos, cumplir con regulaciones y generar confianza en el mercado. Su implementación contribuirá a un ecosistema financiero más seguro, resiliente y confiable.[92]

[91] Federal Office for Information Security (BSI). (2021). *IT Security Act 2.0*. Retrieved from https://www.bsi.bund.de.

[92] NQA, I*SO 27001: 2022 Guía de Implementación de Sistemas de Gestión de Seguridad de la Información* (Reino Unido: NQA, 2022), 4-31.

CAPITULO III: CONCLUSIONES

3.1. Conclusiones

a) En respuesta a la hipótesis general planteada, para que las empresas cumplan eficazmente con la Ley de Protección de Datos Personales, es esencial que inviertan en capacitación continua sobre sus requisitos normativos, garantizando que todo el personal relevante esté debidamente informado. Además, deben ajustar sus sistemas de ciberseguridad a las necesidades específicas de la empresa, considerando los riesgos particulares de su sector. De esta forma, se asegurarán de que las medidas de protección de datos sean efectivas, cumpliendo con la normativa y protegiendo la privacidad de los usuarios.

b) En respuesta a la primera hipótesis específica, advertimos que la falta de capacitación adecuada y de criterios claros sobre las medidas de seguridad exigidas ha generado interpretaciones ambiguas de la normativa, permitiendo que muchas empresas no adopten estándares adecuados para la protección de datos personales. Asimismo, el alto costo asociado a la infraestructura tecnológica y la contratación de especialistas en ciberseguridad representa una barrera significativa para las empresas en crecimiento, lo que las hace más vulnerables a ciberataques y a incumplimientos normativos. Por ello, es fundamental promover incentivos financieros y estrategias de capacitación que faciliten la correcta implementación de la legislación en materia de protección de datos y ciberseguridad.

c) En respuesta a la segunda hipótesis específica, consideramos que la ley debería plasmar de forma explícita y obligatoria los criterios específicos en el artículo 16 y posteriores reglamentos de la norma, considerando el tamaño y capacidad de las empresas, para así fortalecer la Ley de Protección de Datos Personales y mejorar la ciberseguridad en el país. Implementar el ISO 27001 permitirá que nuestro país se alinee con las mejores prácticas internacionales, asegurando una mayor protección de datos personales y disminuyendo los riesgos que están asociados a los ciberataques y divulgación de información.

d) En respuesta a la tercera hipótesis específica, consideramos que efectivamente, el incumplimiento de los parámetros de protección de datos personales que aparecen en la Ley N° 297333, Ley de Protección de Datos Personales, expone a las empresas a

consecuencias jurídicas, operativas y reputacionales. Con el análisis observamos que el incumplimiento de los parámetros normativos pone en riesgo los derechos fundamentales de los titulares de los datos personales, generando como respuesta una responsabilidad administrativa, civil y hasta penal por parte de la empresa o entidad que manipula esta información. Por lo tanto, es necesario un respeto irrestricto del marco normativo existente para evitar la afectación de todas las partes involucradas.

BIBLIOGRAFÍA

Libros:

Arreola , Adolfo. *Ciberseguridad: ¿Por qué es importante para todos?* 1ª ed. Ciudad de México: Siglo XXI Editores, Universidad Anáhuac, 2019.

Bravo, David. *Derecho digital y protección de datos: Retos y oportunidades*. Valencia: Editorial Tirant lo Blanch, 2021.

Cypher, Bennett. *The Right to Be Forgotten: The Role of Personal Data in the Digital Age*. In The Globalization of Privacy, edited by Paul M. Schwartz and Daniel J. Solove. London: Routledge, 2018.

Córtazar, Patricia. *Protección de Datos Personales y Nuevas Tecnologías en Perú*. Lima: Pontificia Universidad Católica del Perú, 2019.

García, Jimena. *Privacidad y Protección de Datos Personales: Retos y Oportunidades en Perú*. Cusco: Universidad Andina del Cusco, 2019.

González, María Jesús. *La legislación de protección de datos en España y su impacto en el sector financiero*. Barcelona: Editorial Online, 2019.

NQA, I*SO 27001: 2022 Guía de Implementación de Sistemas de Gestión de Seguridad de la Información*. Reino Unido: NQA, 2022.

Ortega, José Manuel. *Ciberseguridad: Manual Práctico*. 1ª ed. Bogotá: Ecoe Ediciones, 2024.

Ruiz de BIEE, Javier. *Ciberseguridad y protección de datos en el siglo XXI: Normativa y estándares*. Madrid: Ediciones Jurídicas, 2020.

Salazar, César. *Derechos digitales y protección de datos en el Perú*. Lima: Editorial Jurídica Peruana, 2020.

Santillán, Jorge. *Derecho a la privacidad y protección de datos personales en el Perú* 2020.

Solove, Daniel. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven: Yale University Press, 2007.

Vásquez, Raúl. *Protección de Datos Personales: Un Enfoque desde la Legislación Peruana*. Lima: Editorial Universitaria, 2020.

Artículos de revista académica:

Álvarez, Gonzalo. “La protección de datos personales en el Perú: Análisis crítico de la Ley N° 29733”. *Revista de Derecho Informático*, no. 20 (2019): 45-67.

Arteaga, Mildred. “Smart Contratcs: Perspectivas en la legislación mexicana actual y consideraciones para su aplicación”. *Infotec Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación*, (2023:. 66-67.

Calle, Aldrin, Yaritza Conforme, Emily Magallanes, y Juleidy Guaranda. “Importancia de la Ciberseguridad en la Investigación de Mercados Digital.” *Ciencia y Desarrollo* 27, no. 2 (abril-junio 2024): 256-259.

Córdova, María. “La privacidad y la protección de datos: Derechos y obligaciones en el Perú”. *Anuario de Derecho,* no, 14 (2018): 25-50.

De la Vega, Fernando. “Perspectivas sobre la protección de datos y la privacidad en la era digital”. *Revista de Tecnología y Derecho,* no. 7 (2021): 15-35.

Eguiguren, Francisco. “El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú.” *THĒMIS-Revista de Derecho*, no. 67 (2015)

Zamudio, María. “Reflexiones sobre la observancia del derecho fundamental a la protección de datos personales en diversos actos regulados por el Código Civil”. *Ius et Praxis,* no. 55 (2022).

Nissenbaum, Helen. “Privacy as Contextual Integrity.” *Washington Law Review*, no. 79, (2004): 101-139.

Schwartz, Paul M. “Information Privacy in the Electronic Age.” *Harvard Law Review* 117, no. 7 (2004): 2075-2128.

Artículos en espacios web académicos:

César Piepenburg, Carolina. “Desafíos de la Ciberseguridad en el Sector Financiero.” Intelequia, 1 de agosto de 2024. https://intelequia.com/es/blog/post/desaf%C3%ADos-de-la-ciberseguridad-en-el-sector-financiero.

Conexión ESAN. “Nuevos estándares para la protección de datos personales en el Perú.” Conexión ESAN, 4 de junio de 2024. https://www.esan.edu.pe/conexion-esan/nuevos-estandares-para-la-proteccion-de-datos-personales-en-el-peru.

El Comercio. “Hackeo al Interbank: Indecopi anuncia investigación preliminar contra el Interbank.” El Comercio, 15 de noviembre de 2024. https://elcomercio.pe/lima/hackeo-al-interbank-indecopi-anuncia-investigacion-preliminar-contra-el-interbank-lima-ultimas-noticia/?ref=ecr#google_vignette.

Estudio Echecopar. “Nuevo Reglamento de la Ley de Protección de Datos Personales”. Estudio Echecopar Asociado a Baker & MacKenzie International, 03 de diciembre de 2024, https://www.echecopar.com.pe/publicaciones-nuevo-reglamento-de-la-ley-de-proteccion-de-datos-personales.html

Fernando Montalvão. “Seguridad de la Información y Protección de Datos en el Perú: Una Guía Práctica para Empresas”. Lima: IEP, 2021.

Garrigues. “¿Cómo se regula la protección de datos en Latinoamérica y cómo influye el RGPD?” Garrigues, 02 de diciembre de 2024. https://www.garrigues.com/es_ES/noticia/regula-proteccion-datos-latinoamerica-influye-rgpd

German Montoya, "Hackeo a Interbank evidencia el rol imprescindible de los profesionales de Ciberseguridad - Noticias Trujillo", Noticias Trujillo, 5 de noviembre de 2024, https://noticiastrujillo.pe/hackeo-a-interbank-evidencia-el-rol-imprescindible-de-los-profesionales-de-ciberseguridad/

"Hackeo a Interbank alerta al sector bancario: ¿Estamos seguros?", Blogs Universidad Continental, consultado el 24 de febrero de 2025, https://blogs.ucontinental.edu.pe/hackeo-a-interbank-alerta-al-sector-bancario-estamos-seguros/carreras/ciencia-de-la-computacion/

Infobae. “Robo de datos en Interbank al descubierto: así operó el hacker para sustraer información de clientes del banco”. Infobae, 11 de noviembre de 2024. https://www.infobae.com/peru/2024/11/11/robo-de-datos-en-interbank-al-descubierto-asi-opero-el-hacker-para-sustraer-informacion-de-clientes-del-banco/

LP Pasión por el Derecho. “Minjus inicia proceso sancionador contra el BCP por filtración de datos,” LP Derecho, 4 de diciembre de 2024, https://lpderecho.pe/minjus-inicia-proceso-sancionador-bcp-filtracion-datos/.

Miranda Guzmán, Diego. “Los datos personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado): enfoque, ámbito de aplicación y contenido”. Universidad Externado de Colombia. 02 enero de 2024

https://telecomunicaciones.uexternado.edu.co/los-datos-personales-y-su-regulacion-en-colombia-datos-sensibles-datos-publicos-semiprivado-y-privado-enfoque-ambito-de-aplicacion-y-contenido/

Pizcueta, Pepa. "Ciberseguridad para PYMES: Desafíos y oportunidades." Next Educación, 03 de enero de 2024. https://www.nexteducacion.com/noticias/ciberseguridad-para-pymes-desafios-y-oportunidades/

Redacción Gestión. "Interbank: Fiscalía en Ciberdelincuencia inició diligencias sobre presunto hackeo." *Gestión*, 30 de diciembre de 2024. https://gestion.pe/economia/interbank-hackeo-fiscalia-en-ciberdelincuencia-inicio-diligencias-sobre-presunto-hackeo-indecopi-datos-de-usuarios-noticia/.

Rodrigo, Elias & Medrano Abogados. "Alerta Privacidad y Protección de Datos - Diciembre 2024". Rodrigo, Elias & Medrano Abogados, 22 de febrero de 2025, https://www.estudiorodrigo.com/alerta-privacidad-y-proteccion-de-datos-diciembre-2024/

SBS Informa. Protección de datos personales: cautelando la seguridad de la información de los supervisados, usuarios y ciudadanos. Boletín Semanal N° 03. Febrero 2025. https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1250?title=Protecci%C3%B3n%20de%20datos%20personales:%20cautelando%20la%20seguridad%20de%20la%20informaci%C3%B3n%20de%20los%20supervisados,%20usuarios%20y%20ciudadanos#:~:text=Desde%20hace%2010%20a%C3%B1os%2C%20el,respeto%20de%20los%20dem%C3%A1s%20derechos

Jurisprudencia:

Ministerio de Justicia y Derechos Humanos del Perú, *Resolución Directoral N.º 06-2023-JUS/DGTAIPD-DPDP*, de 13 de enero de 2023.

Normas citadas:

Congreso de la República del Perú. *Ley 29733, Ley de Protección de Datos Personales*. 2011. https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf.

Decreto Supremo N° 016-2024-JUS, de 30 de noviembre. Reglamento de la Ley 29733, Ley de Protección de Datos Personales. (Lima, 30 de noviembre de 2024)

Gobierno de Perú, *Ley N.º 29733, Ley de Protección de Datos Personales* (Lima: Congreso de la República, 2011), https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf.

Ley 29733, de 3 de julio, Ley de Protección de Datos Personales. (Lima, 3 de julio de 2011).

Decreto Supremo N.º 016-2024-JUS, Reglamento, art. 37, inc. 1, num. 2, El Peruano, (Lima, 30 de noviembre de 2024).

Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales, 2013.

Decreto Supremo N° 116-2017-PCM, Directiva de Seguridad de la Información en la Administración Pública, (Lima, 12 de febrero de 2017).

Ley N° 30999, Ley de Gobierno Digital, Lima, 2019.

Decreto Legislativo N.º 1412, Decreto de Gobierno Digital, 2018.

Ley N° 30096, Ley de Delitos Informáticos, 2013.

ANEXO

	GENERAL	ESPECÍFICO 1	ESPECÍFICO 2	ESPECÍFICO 3
PROBLEMA	¿De qué forma la Ley de Protección de Datos Personales en el Perú es eficaz para garantizar la protección de datos personales en los sistemas de ciberseguridad del sector empresarial financiero?	¿Cuáles son las brechas entre el marco normativo de la Ley 29733 y su implementación práctica en los sistemas de ciberseguridad empresarial?	¿Qué factores normativos limitan la eficacia de la Ley 29733 en la protección de datos personales en diferentes segmentos empresariales?	¿Cuáles son las consecuencias jurídicas y operativas del incumplimiento de la Ley 29733 en la seguridad de los datos personales en el ámbito empresarial financiero?
OBJETIVO	Analizar la eficacia de la Ley 29733 en la protección de datos personales a través de los sistemas de ciberseguridad en el sector empresarial financiero.	Identificar y analizar las brechas existentes entre las disposiciones de la Ley 29733 y su implementación práctica en los sistemas de ciberseguridad empresarial.	Evaluar los factores normativos que afectan la eficacia de la Ley 29733 en diferentes segmentos empresariales financieros.	Determinar las consecuencias jurídicas y operativas del incumplimiento de la Ley 29733 en la protección de datos personales en el ámbito empresarial.
HIPÓTESIS	La eficacia de la Ley de Protección de Datos Personales en la implementación de sistemas de ciberseguridad empresarial está condicionada por el nivel de comprensión de sus parámetros normativos y la capacidad de adaptación a las necesidades específicas de cada empresa.	La limitada eficacia en la implementación de sistemas de ciberseguridad se debe principalmente al desconocimiento de los parámetros técnico-normativos de la Ley y los altos costos de implementación para empresas en crecimiento y compromete la seguridad de la información.	La ausencia de criterios específicos en el artículo 16 y 17 de la Ley de Protección de Datos Personales (Ley 29733), que consideren el tamaño y la capacidad operativa de las empresas, junto con la insuficiente capacitación para su implementación, limita significativamente la eficacia en la protección de datos personales en los distintos	El incumplimiento de los parámetros para la protección de datos personales que establece la Ley 29733 exponen a la empresa a consecuencias jurídicas y operativas significativas. En el ámbito legal, la empresa puede enfrentar demandas civiles y responsabilidad penal en caso de delitos informáticos o filtraciones de información. Por otro lado, a nivel

			segmentos empresariales. En ese contexto, la adopción de la norma ISO 27001 proporcionaría un marco estructurado y estandarizado para fortalecer la seguridad de la información, asegurando un cumplimiento más efectivo de la normativa y promoviendo una gestión integral de riesgos en la protección de datos en el país.	operativo, el incumplimiento puede generar vulnerabilidades en los sistemas de seguridad, facilitando la exposición de datos sensibles de trabajadores y clientes, deteriorando la reputación de la empresa.