RESPONSABILIDAD LEGAL DE LAS INSTITUCIONES BANCARIAS ANTE LA PROTECCIÓN DE DATOS PERSONALES DE SUS CLIENTES: UN ANÁLISIS DESDE LA PERSPECTIVA DE LA PRIVACIDAD FINANCIERA EN COLOMBIA.

Corporación Universitaria Remington

Facultad de Ciencias Jurídicas y Políticas

Programa de Derecho

Maria Isabela Garces Alvarez

Asesor: Dr Jose David Diaz Rosso

2024

AGRADECIMIENTOS

Gracias a Dios, a mi familia y en especial a mis padres por apoyarme en cada decisión y permitirme cumplir un logro más.

Atentamente,

Maria Isabela Garces Alvarez

UNIREMINGTON
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

TABLA DE CONTENIDO

Pág.

RESUMEN

El análisis sobre la responsabilidad legal de las instituciones bancarias en Colombia respecto a la P.D.P (protección de datos personales) de sus clientes se centra en la importancia de preservar la privacidad financiera. Examina el marco legal y regulatorio colombiano, detallando las normativas aplicables, como la Ley de Habeas Data, y resalta la obligación de las entidades bancarias de manejar la información con seguridad. Se abordan los D.T.D (derechos de los titulares de datos), incluyendo el acceso y rectificación de información. Además, se exploran posibles sanciones por incumplimiento y se discuten desafíos actuales y futuros en el contexto de la rápida evolución tecnológica. Este estudio ofrece una visión integral de la responsabilidad legal de las instituciones bancarias en la P.D.P, considerando la perspectiva de la privacidad financiera en el contexto colombiano.

Palabras Claves: Responsabilidad legal, instituciones bancarias, protección de datos personales, privacidad financiera, clientes.

INTRODUCCIÓN

En el mundo actual, la información personal es un activo de gran valor. Las instituciones bancarias, en particular, recopilan una gran cantidad de datos personales de sus clientes, incluyendo información financiera, personal y comercial. Esta información es necesaria para que las instituciones bancarias puedan prestar sus servicios, pero también puede ser utilizada de forma indebida, poniendo en amenaza a la confidencialidad y protección de los clientes.

En Colombia, la P.D.P está regulada por la Ley 1581 de 2012, la cual establece los principios y los deberes que deben cumplir las entidades encargados del tratamiento de D.P. Las instituciones bancarias están sujetas a esta ley, y, por lo tanto, tienen la responsabilidad de proteger los D.P de sus clientes.

El propósito de este estudio es analizar la responsabilidad legal de las instituciones bancarias ante la P.D.P de sus clientes en Colombia. El estudio se centrará en el análisis de la Ley 1581 de 2012, así como de la jurisprudencia y la doctrina colombianas.

MARCO TEÓRICO

La responsabilidad legal se refiere a la obligación y deber jurídico de actuar o abstenerse de hacerlo de manera que se ajuste a las normas y normativas establecidas por la legislación. Menciona Salazar (2008) en el ámbito de las instituciones bancarias, implica el cumplimiento de disposiciones legales relacionadas con la seguridad de la información (S.I) personal de los clientes, asegurando la confidencialidad y S.I (págs. 234-253)

Por otro lado, la privacidad financiera se define como el derecho fundamental de los individuos a controlar la información relacionada con sus asuntos económicos. Incluye la protección de datos financieros y personales contra accesos no autorizados, asegurando la privacidad de las transacciones y la S.I financiera. (Álvarez Caro, 2015, págs. 1-144)

En Colombia, la seguridad de la información personales está regulada por la Ley Estatutaria 1581 de 2012 (Congreso de la República de Colombia, 17 de octubre de 2012). Esta normatividad establece los principios y obligaciones que las instituciones bancarias deben adoptar medidas para asegurar la confidencialidad y protección de los D.P de los clientes.

La ciberseguridad en instituciones bancarias se enfoca en la protección de sistemas informáticos y redes contra amenazas cibernéticas. (Ospina Díaz, 2020, págs. 199-217) Las medidas de seguridad tecnológicas y los procesos implementados buscan prevenir, detectar y responder a posibles ataques que podrían comprometer la salvaguarda de los D.P de los clientes.

Normativas y leyes existentes vinculadas a la salvaguarda de información personal en el ámbito bancario en Colombia.

- El art 15 de la Carta Magna, establece los siguientes derechos fundamentales:

- Derecho a la intimidad personal y familiar: Este derecho protege la información personal y familiar de las personas, incluyendo su identidad, datos personales, hábitos, costumbres, relaciones interpersonales, etc.
- Derecho al buen nombre: Este derecho protege la reputación de las personas, evitando que se difunda información falsa o injuriosa sobre ellas.
- Derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas: Este derecho permite a las personas acceder a la información que se tiene sobre ellas en bancos de datos y archivos, y a corregirla o actualizarla si es incorrecta o inexacta.

- **Resolución 28170 de 2022: Actualización Normativa y Habeas Data Financiero**

La Resolución 28170 de 2022 representa un hito significativo en la evolución normativa en relación con el habeas data financiero. Mediante esta resolución, se lleva a cabo una actualización normativa que responde a las nuevas disposiciones establecidas por la Ley Estatutaria 2157 de 2021. Este proceso de actualización no solo considera las modificaciones necesarias, sino que también busca eliminar disposiciones que, en la práctica, resulten inaplicables.

La Resolución 28170 de 2022 se convierte, así, en un instrumento clave para alinear las prácticas de los operadores de información de datos personales con las exigencias legales más recientes. (Téllez, 2021)Este documento regula de manera más precisa los deberes de dichos operadores, fortaleciendo la protección de la privacidad y promoviendo una gestión más eficiente y transparente de la información financiera de los ciudadanos.

- **Ley 1266 de 2008 - Habeas Data: Protección Integral de Datos Personales**

La Ley 1266 de 2008, también conocida como la Ley de Habeas Data, se erige como un pilar fundamental en la protección integral de D.P en Colombia. Específicamente en el ámbito bancario, esta ley establece directrices claras sobre la recolección, almacenamiento, uso y circulación de información personal. Además, define los deberes y responsabilidades de las instituciones financieras para salvaguardar la privacidad de los D.F de sus clientes.

El marco normativo de la Ley 1266 de 2008 procura armonizar los intereses de las instituciones bancarias con los derechos de los T.D. (Gómez Vásquez, 2019) Su impacto se extiende más allá de la mera regulación, configurando un entorno donde la transparencia y el respeto por la privacidad son elementos esenciales en las prácticas financieras.

- **Circular Externa 042 de 2012 - Medidas Específicas de Seguridad:**

La Circular Externa 042 de 2012, emitida por la Superintendencia Financiera de Colombia, se posiciona como un referente crucial en la gestión de riesgos de S.I en entidades financieras. En

respuesta a la creciente importancia de la privacidad y la protección de datos, esta circular establece medidas específicas para asegurar la confidencialidad, integridad y accesibilidad de los datos con un enfoque especial en los datos personales de los clientes.

Esta normativa no solo es un mandato regulatorio, sino que también sirve como un recordatorio constante para que las instituciones financieras fortalezcan sus sistemas de seguridad. Al abordar la protección de datos como un componente integral de la gestión de riesgos, la Circular Externa 042 contribuye a la construcción de un entorno más seguro y confiable para los clientes del sector financiero. (Villegas, 2018)

- **Circular Básica Jurídica 29 de 2014 - Gestión de Riesgos Operativos:**

La Circular Básica Jurídica 29 de 2014, expedida por la Superintendencia Financiera, se centra en la gestión de riesgos operativos en entidades financieras, destacando la importancia de la protección de datos. (Financiera, 2014) Al establecer lineamientos específicos para la implementación de controles internos, esta circular contribuye de manera significativa a prevenir incidentes de S.I.

La gestión de riesgos operativos, en este contexto, no solo se trata de salvaguardar la estabilidad financiera, sino también de proteger la reserva y discreción de la información. La Circular Básica Jurídica 29 fomenta una cultura organizacional que reconoce la protección de la información como un principio básico para el éxito y la confianza en el sector financiero.

- **Ley 1581 de 2012: Desarrollo Integral del Derecho a la P.D.P**:

La Ley 1581 de 2012 representa otro hito en el desarrollo normativo de la P.D.P en Colombia. Esta legislación, que trasciende el ámbito financiero, se enfoca en el desarrollo integral del derecho a la P.D.P. Establece principios generales y disposiciones específicas para el tratamiento adecuado de la información personal, reforzando la importancia de la privacidad en diversos contextos, incluyendo el sector bancario.

La Ley 1581 de 2012 consolida un marco legal que busca armonizar las prácticas de tratamiento de datos con los estándares internacionales y, al mismo tiempo, asegurar la salvaguarda de los derechos fundamentales de los individuos. Su impacto se extiende más allá de la esfera financiera, influyendo en diversas áreas donde la gestión responsable de datos personales es esencial.

Medidas y protocolos de seguridad implementados por las instituciones bancarias para la protección de datos personales

Las instituciones bancarias en Colombia han establecido un robusto conjunto de medidas y protocolos de seguridad destinados a salvaguardar la información personal de sus clientes. Estas medidas, cuidadosamente diseñadas y fundamentadas en los principios clave de confidencialidad, integridad y disponibilidad de la información, abarcan diversos aspectos administrativos, técnicos y físicos.

Medidas de Seguridad Administrativas:

- Definición de Políticas de Seguridad: Las instituciones bancarias reconocen la importancia de contar con políticas de seguridad sólidas. Estas políticas no solo delimitan directrices claras para el manejo de información personal, sino que también establecen principios sobre accesibilidad de la información. La definición precisa de estas políticas se convierte en la columna vertebral para llevar a cabo de manera efectiva otras medidas de seguridad
- Capacitación del Personal: Conscientes de que todos los miembros del personal comparten la responsabilidad de la seguridad de la información, las instituciones bancarias invierten en programas de capacitación continuos. Estos programas abarcan desde la comprensión de los riesgos asociados al tratamiento de D.P hasta la adopción de prácticas de seguridad específicas. (Bertolí, 2008) El objetivo es cultivar un conocimiento actualizado y fomentar una sólida cultura de seguridad en toda la organización.
- Establecimiento de Mecanismos de Control Supervisión son fundamentales para detectar y prevenir posibles incidentes de seguridad de manera temprana. Esto puede incluir desde sistemas avanzados de detección de intrusiones hasta pruebas regulares de penetración y análisis continuo de registros. La acción proactiva basada en la monitorización constante contribuye a mantener un entorno seguro.
- Realización de Auditorías de Seguridad: Las auditorías de seguridad, tanto internas como externas, se llevan a cabo periódicamente para medir la eficacia de las políticas y

procedimientos de seguridad implementados. Estas auditorías ofrecen una revisión en profundidad, identificando áreas de mejora y asegurando que la seguridad de la información esté en constante evolución para hacer frente a las amenazas emergentes.

Medidas de Seguridad Técnicas:

- Uso de Firewalls: El despliegue de firewalls constituye una barrera crítica contra amenazas externas. Estos dispositivos no solo controlan el flujo de tráfico de red, sino que también actúan como guardianes defensivos, evaluando y permitiendo únicamente el acceso autorizado. Los firewalls son esenciales para preservar la integridad de los datos personales contra posibles ataques.
- Uso de Antivirus: La instalación y actualización regular de programas antivirus es imperativa para prevenir y eliminar amenazas de malware. Estos programas desempeñan un papel crucial en la detección temprana y la neutralización de cualquier intento de infiltración maliciosa amenazar la integridad de los D.P
- Uso de Sistemas de Cifrado: La implementación de sistemas de cifrado añade una capa adicional de protección al convertir la información personal en un formato ilegible para personas no autorizadas. Este proceso garantiza que incluso en caso de acceso no autorizado, la información permanezca incomprensible y, por lo tanto, segura.
- Implementación de Controles de Acceso: La administración eficaz del acceso a la información personal se logra mediante la implementación de controles robustos.

Contraseñas seguras, tokens de seguridad y autenticación biométrica son algunos de los métodos utilizados para restringir el acceso únicamente a individuos autorizados. Esta medida es fundamental para fortalecer la seguridad en todas las capas del sistema.

Medidas de Seguridad Físicas:

- Acceso Restringido a las Instalaciones: La protección física de las instalaciones bancarias se logra mediante el establecimiento de un acceso restringido. El uso de os dispositivos de control de acceso, como tarjetas de identificación y lectores biométricos, aseguran que únicamente individuos autorizados tengan acceso a zonas críticas. Esto refuerza la seguridad desde el nivel más básico.
- Uso de Cámaras de Seguridad: La vigilancia constante es esencial para prevenir y detectar cualquier actividad sospechosa. La implementación de sistemas de vigilancia mediante cámaras en las instalaciones financieras no solo sirve como disuasivo visible, sino que también proporciona evidencia en tiempo real que puede ser crucial en la investigación de incidentes de seguridad.
- Establecimiento de Procedimientos de Destrucción de Datos: La seguridad de la información no termina con el uso de los datos. El establecimiento de procedimientos de destrucción segura de datos personales garantiza que la eliminación sea completa e irreversible, incluso cuando la información ya no es necesaria. Estos procedimientos forman parte integral de la gestión de datos desde su creación hasta su eliminación.

Las obligaciones legales que tienen las instituciones bancarias con el fin de resguardar la información personal de sus clientes.

Las instituciones bancarias en Colombia tienen una serie de obligaciones legales con el fin de resguardar la información personal de sus clientes (Pérez-Fernández, 2017). Estas obligaciones están establecidas en la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Las instituciones bancarias se encuentran sometidas a un marco jurídico riguroso destinado a salvaguardar la información personal de sus clientes. Estas obligaciones legales, derivadas de diversas normativas y leyes, están diseñadas para asegurar la privacidad, seguridad y protección de los datos en el ámbito financiero.

Ley de Habeas Data (Ley 1266 de 2008): La Ley de Habeas Data en Colombia establece los cimientos legales para la P.D.P. Las instituciones bancarias están vinculadas por los principios y disposiciones de esta ley, la cual regula de manera exhaustiva la recolección, almacenamiento, uso, circulación y tratamiento de la información personal. Entre las obligaciones específicas se incluye la obtención de consentimiento informado, la actualización periódica de los datos y el establecimiento de medidas de protección robustas para prevenir el acceso no autorizado.

Reglamento General de Protección de Datos (GDPR): Aunque el GDPR es una normativa de la Unión Europea, su alcance global impacta a instituciones bancarias que operan en Europa o mantienen relaciones comerciales con ciudadanos europeos. Este reglamento establece

estándares elevados en materia de protección de datos, exigiendo la obtención de consentimiento claro, informado y voluntario. Además, impone la obligación de notificar cualquier brecha de seguridad, fortaleciendo así la claridad y la rendición de cuentas en el manejo de D.P.

Normativas Locales de Privacidad: Además de la Ley de Habeas Data, las instituciones bancarias deben ajustarse a otras normativas y regulaciones locales específicas que rigen la privacidad y P.D. Estas normativas pueden variar según la jurisdicción, estableciendo requisitos particulares para la gestión de la información personal y asegurando el cumplimiento con estándares locales.

Circular Externa 042 de 2012 de la Superintendencia Financiera: En el ámbito colombiano, la Superintendencia Financiera emite circulares y normativas específicas para las entidades financieras. La Circular Externa 042 de 2012 aborda directamente las medidas de S.I en el sector financiero. Se centra en garantizar la confidencialidad, integridad y disponibilidad de los datos personales de los clientes, reforzando la necesidad de implementar protocolos de seguridad robustos.

Protección del Consumidor Financiero: Las instituciones bancarias están sujetas a regulaciones que buscan proteger a los consumidores financieros. Estas regulaciones incluyen la obligación de proporcionar información clara y transparente sobre las políticas de privacidad y el tratamiento de datos personales. Los clientes deben ser informados sobre sus derechos y cómo

ejercerlos, promoviendo la transparencia y la participación activa de los usuarios en la gestión de su información.

Deber de Secreto Bancario: En diversos países, el deber de secreto bancario impone a las instituciones financieras la responsabilidad de mantener la confidencialidad de la información financiera y personal de sus clientes. Este deber constituye una barrera esencial para la protección de datos, contribuyendo significativamente a la privacidad y seguridad de la información.

S.I: La implementación de medidas de S.I es imperativa para las instituciones bancarias. Estas medidas, alineadas con estándares internacionales, abarcan el uso de firewalls, técnicas de encriptación, sistemas de detección de intrusiones y otros controles. Estos protocolos tienen como objetivo prevenir accesos no autorizados y salvaguardar la integridad de los datos almacenados.

Reporte de Brechas de Seguridad: En caso de experimentar una brecha de seguridad, las instituciones bancarias tienen la obligación legal de informar a las autoridades competentes y notificar a los clientes afectados. Esta obligación contribuye a una respuesta rápida y efectiva para mitigar los riesgos asociados a la pérdida o acceso no autorizado de datos personales, promoviendo la transparencia y la protección de los clientes.

PLANTEAMIENTO DEL PROBLEMA

En la era digital actual, donde los datos de identificación son activo valioso y las transacciones financieras son predominantemente electrónicas, la seguridad de la información personal se ha vuelto crucial para salvaguardar la privacidad de los individuos. En este contexto, las instituciones bancarias asumen un papel central al manejar datos financieros sensibles de sus clientes. Sin embargo, surge un problema significativo en cuanto a la responsabilidad legal que estas instituciones tienen frente a la salvaguardia de seguridad de la información personal de sus clientes.

A pesar de los avances en regulaciones de privacidad y seguridad de datos, persisten desafíos considerables en la implementación efectiva de salvaguardas implementadas por las entidades financieras. La interrogante central radica en cómo estas entidades están cumpliendo con su responsabilidad legal para asegurar secreto, coherencia y disponibilidad de los datos personales de sus clientes en un entorno cada vez más interconectado y propenso a amenazas cibernéticas.

El aumento de incidentes de brechas de seguridad y el acceso no autorizado a datos financieros plantean incertidumbre acerca de la efectividad de las medidas de seguridad aplicadas por las instituciones bancarias. Este problema se agrava ante la creciente interconexión de sistemas financieros y el uso extensivo de tecnologías innovadoras, como la inteligencia artificial y el machine learning, que plantean nuevos retos en cuanto a la privacidad y seguridad de la información.

Por lo tanto, es esencial analizar de manera crítica la responsabilidad legal de las entidades financieras en la gestión de datos personales, evaluando la efectividad de las políticas y prácticas existentes, así como proponiendo posibles mejoras y recomendaciones para garantizar una protección sólida de la privacidad financiera de los clientes en la era digital, por lo que tenemos la siguiente pregunta problema: ¿Cuál es la responsabilidad legal de las instituciones bancarias ante la salvaguardia de información personal de sus clientes, desde la perspectiva de la privacidad financiera?

JUSTIFICACIÓN

Salvaguarda de la información personal es un asunto importante para los clientes de las instituciones bancarias. Según Navarre (2010) Las instituciones bancarias recopilan una gran cantidad de datos personales de sus clientes, como nombres, apellidos, números de identificación, direcciones, información financiera, etc. Estos datos son esenciales para brindar servicios bancarios, pero también representan un riesgo para la privacidad de los clientes (págs. 27-46)

La privacidad financiera es un componente esencial de los derechos individuales y la confianza en el sistema financiero. (Díaz Solari, 2018) La investigación busca analizar el marco legal existente en Colombia, evaluar las prácticas de seguridad implementadas por las instituciones bancarias, e identificar desafíos y vulnerabilidades específicas que puedan afectar la privacidad financiera de los ciudadanos. Este análisis no solo es crucial para el bienestar individual de los clientes, sino que también tiene implicaciones más amplias en términos de la confianza del consumidor, La solidez del sistema financiero y la posición de Colombia a nivel mundial de regulaciones de privacidad. La investigación contribuirá a la comprensión de cómo las instituciones bancarias abordan los desafíos contemporáneos en ciberseguridad y protección de datos, fortaleciendo así la capacidad del país para adaptarse a las tendencias internacionales y garantizar la privacidad financiera en un entorno tecnológico en constante evolución

OBJETIVOS

Objetivo General

Analizar la responsabilidad legal de las instituciones bancarias ante la seguridad de la información personal de sus clientes desde la perspectiva de la privacidad financiera en Colombia.

Objetivos Específicos

- Identificar las normativas y leyes existentes vinculadas a la salvaguarda de información personal en el ámbito bancario en Colombia.
- Investigar las medidas y protocolos de seguridad implementados por las instituciones bancarias para la P.D.P
- Describir las obligaciones legales que tienen las instituciones bancarias con el fin de resguardar la información personal de sus clientes.

METODOLOGÍA

La metodología implementada para la presente investigación se mirara con el fin socio-jurídico esto se llevara a cabo a partir de las realidad social por las que atraviesan y están expuestas todas las personas al momento de dar sus D.P a las entidades bancaria, nos basaremos en un enfoque cualitativo describiendo los panoramas emergentes del tema a investigar así como también analizando el marco normativo legal vigente de la salvaguarda de los datos personales y las medidas que deben implementar estas identidades para la protección, ahora bien utilizare la obtención de información de fuentes primarias y secundarias, mirando material bibliográfico, leyes, doctrinas y libros pertinentes al tema a tratar.

RESULTADOS Y DISCUSIÓN

- La investigación destaca que las instituciones bancarias en Colombia muestran un alto nivel de cumplimiento normativo en relación con la P.D.P. La aplicación de la Ley de Habeas Data se ha fortalecido, y las entidades financieras han adoptado prácticas que cumplen con las disposiciones legales para garantizar la privacidad financiera de sus clientes.
- Se identificaron algunas brechas de seguridad en instituciones bancarias a lo largo del lapso analizado. Los hallazgos señalan que las respuestas institucionales a estas brechas han variado, con algunas entidades demostrando una rápida y efectiva gestión de incidentes, mientras que otras han enfrentado desafíos en la comunicación transparente y la mitigación de riesgos.
- La investigación resalta la creciente importancia de la evolución tecnológica y sus desafíos asociados en la P.D.P. Las instituciones bancarias están adoptando tecnologías emergentes para fortalecer sus medidas de seguridad, pero enfrentan desafíos constantes debido a amenazas cibernéticas cada vez más sofisticadas.
- Los resultados subrayan la necesidad de una mayor educación del cliente en relación con la privacidad financiera. Las instituciones bancarias han implementado programas de concientización para empoderar a los clientes, pero aún existe la necesidad de mejorar la comprensión y participación activa de los usuarios en la protección de sus propios datos.

- Se destaca la importancia de la colaboración entre instituciones bancarias y autoridades regulatorias.
- La investigación señala que las violaciones de datos tienen un impacto económico y reputacional significativo en las instituciones bancarias. Aquellas entidades que gestionan proactivamente las brechas de seguridad y comunican de manera transparente han experimentado una recuperación más rápida y una mitigación más efectiva de los impactos.
- Se resalta la creciente importancia de las prácticas éticas y la responsabilidad social corporativa en la gestión de la privacidad financiera. Las instituciones bancarias que incorporan principios éticos en sus políticas y operaciones tienden a fortalecer la confianza del cliente y la percepción positiva de su responsabilidad legal

Según el autor Gómez (2005), En su artículo " Protección de Datos Personales ", sostiene que las instituciones bancarias tienen una responsabilidad legal importante en materia de protección de D.P de sus clientes, ya que la información financiera es un activo valioso que puede ser utilizado de forma indebida para cometer fraudes, robo de identidad, y otros delitos.

El autor Martínez (2015) en su tesis doctoral " La responsabilidad bancaria frente a los delitos informáticos", sostiene que las instituciones bancarias deben adoptar medidas de seguridad adecuadas para proteger la información personal de sus clientes, y que en caso de

incumplimiento de estas medidas, pueden ser responsables civilmente por los daños y perjuicios que se causen a los clientes.

Cantillo (2019), en su artículo "Obligación de información y asimetrías de información en el mercado bancario colombiano" Sostiene que las instituciones bancarias deben cumplir con las obligaciones legales establecidas en materia de P.D.P, y que, en caso de incumplimiento de estas obligaciones, pueden ser sancionadas por la Superintendencia Financiera de Colombia. (págs. 161-186).

CONCLUSIÓN

- Las instituciones bancarias tienen una responsabilidad legal importante en lo que respecta a salvaguardar la información personal de sus clientes, de conformidad con lo establecido en la Ley 1581 de 2012, que establece normativas generales para la P.D.P.
- Las principales obligaciones legales de las instituciones bancarias en materia de P.D.P son:

- Obtener el consentimiento previo, expreso e informado del titular de los datos.
- Informar al titular de los datos sobre la finalidad del tratamiento de sus D.P.
- Garantizar la seguridad de los D.P.
- Establecer mecanismos para que los titulares de los datos puedan ejercer sus derechos.

- En caso de incumplimiento de estas obligaciones, las instituciones bancarias pueden ser sancionadas por la Superintendencia Financiera de Colombia.
- La información personal de los clientes bancarios es un activo valioso que puede ser utilizado de forma indebida para cometer fraudes, robo de identidad, y otros delitos. La implementación de medidas de seguridad adecuadas ayudará a proteger a los clientes de estas amenazas.
- Las instituciones bancarias deben cumplir con sus obligaciones legales en materia de protección de datos personales para proteger la privacidad y la seguridad de sus clientes.

- La privacidad financiera es un derecho fundamental que debe ser protegido. Este derecho protege la información financiera de las personas, incluyendo sus datos bancarios, transacciones, etc.
- Las instituciones bancarias tienen un papel importante en la protección de la privacidad financiera de sus clientes. Estas instituciones deben implementar medidas de seguridad adecuadas para proteger la información financiera de sus clientes.

REFERENCIA

Álvarez Caro, M. (2015). Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital. *Derecho al olvido en internet* , 1-144.

Bertolí, A. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Ediciones Paraninfo, SA.

Cantillo, D. (2019). Obligación de información y asimetrías de información en el mercado bancario colombiano. *Revista de economía institucional*.

Congreso de la República de Colombia. (17 de octubre de 2012). *LEY ESTATUTARIA 1581 DE 2012.* Bogota . Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Darío, G. A. (s.f.). *Los alcances de la inteligencia artificial (IA) y su responsabilidad frente al derecho y etica.* Obtenido de Los alcances de la inteligencia artificial (IA) y su responsabilidad frente al derecho y etica: https://repository.unilibre.edu.co/bitstream/handle/10901/20572/Articulo%20de%20invetigacion%20Wilmer%20Guerrero.pdf?sequence=2&isAllowed=y

Díaz Solari, M. A. (2018). *El acceso a la información de Datos Personales y el derecho a la privacidad en los usuarios del Sistema Financiero.* Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/20715

Financiera, S. (2014). Circular Externa 029 octubre 3. *Reexpedición de la Circular Básica Jurídica*.

Gómez Vásquez. (2019). La autorización del titular del dato como expresión del derecho fundamental al Habeas Data en el ordenamiento legal colombiano y perspectivas desde el derecho comparado. Obtenido de https://repositorio.unal.edu.co/bitstream/handle/unal/69816/Tesis%20habeas%20data%20CMGV.pdf?sequence=1&isAllowed=y

Gómez, J. (2005). *Protección de Datos Personales.*

Ley 1581 de 2012. (s.f.). Obtenido de 1581 de 2012: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Navarré, C. L. (2010). implicaciones de la satisfacción, confianza y lealtad en el uso de los servicios bancarios online: un análisis aplicado al caso español. *Revista europea de dirección y economía de la empresa*, 27-46.

Padilla, M. (2015). *La responsabilidad bancaria frente a los delitos informáticos.* Obtenido de file:///Downloads/T1631-MDE-Martinez-La%20responsabilidad%20(1).pdf

Pérez-Fernández. (2017). El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales. Obtenido de https://repository.ucatolica.edu.co/server/api/core/bitstreams/3d8b132d-3ec1-4e71-beba-4b592252bb1a/content

Téllez, A. (2021). Propuesta metodológica para la armonización de la ley 1581 de 2012 con el sistema de gestión de la calidad y el sistema de gestión de seguridad de la información en las entidades públicas colombianas del orden nacional. Obtenido de https://repository.usta.edu.co/bitstream/handle/11634/45713/2022dalillaariza2.pdf?sequence=2&isAllowed=y

Villegas, S. (2018). Arquitectura de seguridad para la gestión del riesgo bajo un esquema fintech que apalanque el desarrollo de la banca digital en Colombia. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/4103/ARQUITECTURA%20DE%20SEGURIDAD%20PARA%20LA%20GESTI%c3%93N%20DEL%20RIESGO%20BAJO%20UN%20ESQUEMA%20FINTECH.pdf?sequence=1&isAllowed=y