

# Una mirada jurídica a la seguridad informática y hábeas data en el ámbito financiero colombiano.

## A legal view of cyber security and habeas data in the Colombian financial field.

### RESUMEN

Este artículo aborda el análisis de la de los indicadores y herramientas establecidas por la Superintendencia de Industria y Comercio con fin las ventajas y desventajas que se presentan con respecto a que el ciudadano acepte la política de tratamiento de datos de cada entidad bancaria y financiera al adquirir un servicio.

Considerar la importancia para las instituciones financieras recopilar, consultar y proporcionar información sobre sus clientes y clientes potenciales, los llamados "consumidores financieros", deben tener en cuenta factores y aspectos clave que son importantes y relevantes para la gestión información, es decir, datos personales del cliente, por lo que en este sentido Los derechos de los consumidores de servicios financieros están plenamente garantizados la información sobre ellos está contenida en todas las bases de datos.

Al aceptar los términos estipulados por entidades financieras como un banco o una cooperativa, sobre el tratamiento de los datos personales, el usuario adquiere los servicios por parte de dicha entidad, pero a su vez, esta adquiere la responsabilidad de salvaguardar dichos datos y llevar un registro claro de ellos brindando un tratamiento integral el cual se debe presentar como reporte ante la Superintendencia de industria y comercio, con el fin de llevar un control con base en la ley 1581 de 2002 y la ley 1266 de 2008; Así mismo el uso indebido de dicha información conlleva a sanciones estipuladas en el art 19 ley 1266 de 2008.

**En el mundo actual, vivimos en una era digital, en la cual internet es una herramienta fundamental y muy eficaz para establecer una mayor conexión entre las personas, facilitando la comunicación, el acceso a la información en diversos ámbitos y optimizando además la rapidez y efectividad de la adquisición de bienes y servicios entre los usuarios. Por esta razón las corporaciones y empresas que intentan estar a la vanguardia, se han esforzado por entender y hacer uso de esas herramientas que brinda internet. Es por este motivo, por lo que las entidades bancarias por ejemplo, migran a la era digital, creando mecanismos de interacción para sus usuarios, utilizando inteligencia artificial para vender sus productos y que el proveedor acceda a los mismos.**

**PALABRAS CLAVE:**

**DATOS PERSONALES; ENTIDADES BANCARIAS; ESTADO; PROTECCIÓN DE DATOS; SANCIÓN**

**ABSTRACT**

**The current article deals with the analysis of the indicators and tools established by the Colombian Superintendency of Industry and Commerce in order to determine the advantages and disadvantages that come to citizens about accepting the data processing policy of each bank and financial entity when purchasing a service.**

**Consider the importance for financial institutions to collect, consult and provide information about their clients and potential clients, the so-called "financial consumers", they must take into account key factors and aspects that are important and relevant for the management of information, that is, data personal information of the client, so in this sense the rights of consumers of financial services are fully guaranteed the information about them is contained in all the databases.**

**By accepting the terms stipulated by the entity on the treatment of personal data, the user acquires the services by the entity, but in change, it acquires the responsibility to safeguard the data and keep a clear record of them, providing integral treatment which must be presented as a report to the Superintendency of Industry and Commerce, in order to carry out a control based on Law 1581 of 2002 and Law 1266 of 2008;**

**Likewise, the improper use of personal data information leads to sanctions stipulated in article 19, law 1266 of 2008.**

**The world plunged into a digital age, social networks, communications, the internet; That is why banking entities migrate to the digital age by creating algorithms of interaction for their users, that is, they use artificial intelligence to sell their products and that the provider accesses them.**

#### **KEY WORDS**

**BANKING INSTITUTIONS -PERSONAL DATA - DATA PROTECTION - SANCTION - STATE.**

### **INTRODUCCIÓN**

La tecnología a través del paso del tiempo se ha convertido en un elemento fundamental en diversos aspectos de la vida cotidiana, específicamente para las empresas en la creciente transformación que depara el día a día, donde diariamente se presenta la necesidad de la rapidez y la eficiencia utilizando todos los medios que ofrece la tecnología, con ello se presentan nuevas oportunidades: el fácil y rápido acceso a la información, la conexión e interactividad entre los usuarios a través de las redes sociales, la práctica y eficaz variedad de servicios que se pueden brindar de manera virtual por parte de una compañía cualquiera a su clientela, entre otros. En este sentido, estos recursos tecnológicos sirven para que las diferentes empresas ofrezcan mayor productividad, con el desarrollo de procesos óptimos, mejorando su rendimiento, generando más acceso a la comunicación, logrando una gran competitividad en el mercado.

En el desarrollo de la implementación de las nuevas tecnologías por parte de las entidades que ofrecen sus distintos productos, surge la necesidad de expandir su alcance público a través de

los recursos digitales que proporciona internet, tales como páginas web, redes sociales y aplicaciones. De este modo se logra propagar la información de forma masiva para llegar a más usuarios de manera más rápida y con mayor eficacia, evitando así que las personas tengan que desplazarse hasta los puntos de atención físicos, disminuyendo la aglomeración de gente.

En ese contexto, las entidades bancarias y financieras, buscan en la actualidad estrategias tales como líneas de atención al cliente en directorios electrónicos, el acceso a sus productos a través de sus portales web, el chat digital, marketing en redes sociales y las aplicaciones en las tiendas digitales, para llegar al usuario de una forma más eficiente, ágil y oportuna. De esta manera, se optimiza el acceso al portafolio de servicios de las entidades bancarias, agilizando los procesos para solicitudes y estudios de créditos, consulta en centrales de riesgo, realizar transacciones, trámites como consulta de saldo y consignaciones, entre otros.

A raíz de los grandes avances tecnológicos, a los cuales se están acoplando todas las instituciones y empresas que brindan sus distintos servicios, es evidente que la legislación colombiana debe proponer nuevos estatutos que contemplen una normativa que esté a tono con la era virtual que vivimos para regular los límites que debe manejar las diferentes entidades del país con el uso de la tecnología. Es menester que la ley colombiana se actualice, para evitar los vacíos legales a la hora de que aparezcan diversos conflictos entre las compañías y los usuarios en el ámbito mencionado. Es por esto que la Corte Constitucional se da a la tarea de suplir la necesidad de regular de manera integral el poder informático, expidiendo la Ley Estatutaria 1266 de 2008 por medio de la cual se logró regular parcialmente el tema y que para este artículo puntualmente se utilizará a modo de ley ESPECIAL, el cual tiene por objeto

*“(..) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países” (..)*

Ahora, para el año 2012 se expide la ley estatutaria 1581, la cual regula de manera GENERAL la protección de datos personales, tiene por objeto:

*“(..)desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma(...)”*

El artículo 15 de la Constitución Política de Colombia, surge por la trascendencia e impacto para la sociedad ya que señala los mecanismos que permiten a los ciudadanos proteger la integridad, confidencialidad y disponibilidad de la información que suministran en entidades bancarias y financieras, al acceder a servicios en las plataformas de las mismas, ya que el desconocimiento de la trascendencia que se tiene con respecto al uso que se le puede dar a los datos personales, a su uso inadecuado trae consecuencias jurídicas y morales.

Las consecuencias jurídicas y morales, se basan en unos principios internacionales los cuales se mencionan a continuación:

Principio uno: Finalidades Legítimas y Lealtad

Principio dos: Transparencia y Consentimiento

Principio tres: Pertinencia y Necesidad

Principio cuatro: Tratamiento y Conservación Limitados

Principio cinco: Confidencialidad

Principio seis: Seguridad de datos

Principio siete: Exactitud de los Datos

Principio ocho: Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Principio nueve: Datos personales sensibles

Principio Diez: Responsabilidad

Principio once: Flujo Transfronterizo de Datos y Responsabilidad

Principio doce: Excepciones

Principio trece: Autoridades de Protección de Datos (OEA, 2021)

En ese orden de ideas, es esencial enmarcar este artículo con los objetivos de desarrollo sostenible propuestos por las Naciones Unidas, puntualmente con el objetivo número 12, el cual habla sobre la producción y consumo responsables, el tratamiento de datos es fundamental para todos los aspectos de consumo que el hombre enfrenta cada día, por otro lado, el buen uso de la información por parte de las entidades da certeza, confiabilidad, veracidad de la persona. Salvaguardar los datos disminuye el fraude, la estafa entre otras conductas que son contrarias al buen entorno de la sociedad.

En el presente documento se examina bajo qué parámetros es seguro suministrar información personal a las entidades bancarias para los diferentes trámites y servicios que estas prestan. En otras palabras, lo que se pretende es proporcionar al usuario cuáles son las condiciones necesarias y adecuadas para proporcionar datos personales y privados a través de aplicaciones y sitios web que piden esto como requerimiento, con el fin de proteger el derecho fundamental que establece el ART 15 de la Constitución Política de Colombia, donde estipula que “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y que el Estado debe respetarlos y hacerlos respetar”, de igual manera, en la ley 1266 de 2008 y la ley 1581 de 2012 se desarrolla el derecho fundamental anteriormente mencionado, el cual, es el núcleo esencial del artículo.

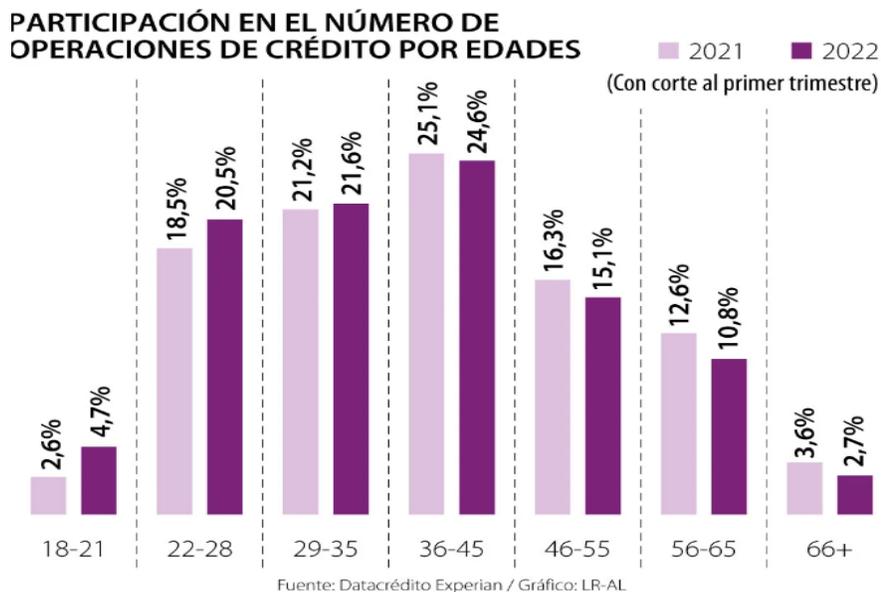
Colombia entró en una era digital, y el mundo jurídico avanza paralelamente con ello, a tal punto de regular el procedimiento, sanciones, ámbito de aplicación de la información de cada ciudadano que figura en un banco de datos, que de transgredir la misma tendrá consecuencias jurídicas y aplica para cualquier rama del derecho, todo contiene información personal, en este caso del demandado y del demandante, del actor y del accionado y deberá ser custodiada y protegida.

**Descripción del problema:** Según el último estudio realizado por datacredito-experian, en el periodo comprendido de enero-marzo 2022, refleja que para el año en curso la solicitud de crédito en la población colombiana aumentó en un 20,8%, teniendo en cuenta los otros años de investigación, debido que este análisis se ha hecho anualmente a su vez categoriza las operaciones

de crédito de la siguiente manera, de acuerdo al género, se evidencia que las mujeres tienen más participación, por otro lado, respecto a la edad, las personas menores de 35 años tienen más interés en construir vida crediticia y adquirir crédito; en el aspecto regional se muestra el Caribe, Cundinamarca y el Eje cafetero, sobresalen como las regiones con mayor actividad crediticia. Por último, respecto al estrato socioeconómico, se evidencia que los estratos 1, 2 y 3 prevalecen al contrastarse con estratos más altos como el 4, 5 y 6, siendo el estrato 3 más activo en la actividad crediticia. El presente trabajo se enfoca principalmente en las primeras tres clases sociales anteriormente mencionadas.

A continuación, se muestran, gráficos con sus estadísticas para así demostrar lo anteriormente mencionado.

Personas entre 18 y 35 años concentraron 46,8% de los créditos en el primer trimestre



Normalmente los clientes de los bancos suelen pedir créditos, en su mayoría, de libre inversión, adquisición de vivienda y tarjetas de crédito, entre otros. Esto quiere decir, que las personas en su afán o premura de adquirir algunos de estos servicios, aceptan los términos y

condiciones que establece la entidad, sin analizar previamente los derechos que le están otorgando a la compañía que les presta el dinero, es decir, no se informan bien al pasar de largo la información legal suministrada en los formularios que diligencian.

**TARJETAS DE CRÉDITO VS. CRÉDITOS ROTATIVOS**

**ESTADO DE LAS TASAS DE CRÉDITOS DE CONSUMO**

\*Corte al cierre de diciembre      \*\*Orden de menor a mayor por valor de la tasa

Tasa crédito rotativo			Tasa tarjeta de crédito	
	11,41%			17,51%
	11,51%	Crédito dinero extra		18,96%
	11,68%	Crédito Cupo Rotativo		19,77%
	12,22%	Crédito de Libre Destino		20,70%
	12,47%			22,28%
	12,83%	Crédito de Libre Inversión		22,60%
	13,90%	Cupoactivo		
	14,05%	Credinsumos		

Fuente: Superfinanciera

**Una mirada jurídica a la seguridad informática y el derecho de hábeas data en el contexto financiero colombiano.**

La Constitución de 1991, aportó algunos estatutos significativos respecto a los derechos fundamentales, que serán salvaguardados por el estado, creando mecanismos que los protejan. A medida que evoluciona el colectivo en sí, con el uso de la tecnología, surgen problemáticas referentes al tratamiento de datos personales de los usuarios por parte de aplicaciones y portales web que pertenecen a diversas compañías que prestan diferentes servicios. Los conflictos que se

pueden dar por la mala manipulación de información privada por parte de cualquier entidad, respecto a sus clientes, deben ser resueltos por estatutos legales que estén en contexto con aspectos de esa naturaleza. En este sentido, por ejemplo, se puede mencionar el ART 15 de la carta magna, que establece el buen nombre, intimidad personal, entre otras. Esa es una de las normas que protege a los individuos y que se ve transgredida regularmente, por las empresas que trabajan con la información que suministran sus usuarios. Es por ello que la sociedad trasciende a una era digital donde la información es más asequible para el ser humano, entre ella, la información personal, si bien es cierto cada persona tiene una identidad, dirección, teléfono, estado civil, capacidad financiera, historia laboral, certificados de estudio, donde toda esta información es accesible en internet y se requiere para negocios de diferente naturaleza.

De acuerdo a lo mencionado anteriormente, el manejo de la información personal o Habeas Data, debe ser regulado y vigilado para garantizar que las diferentes entidades bancarias en este caso, no expongan esos datos privados a personas inescrupulosas que puedan cometer suplantación, fraude, estafa entre otras malas conductas que tiene el Código Penal tipificadas.

Actualmente las entidades bancarias han desarrollado por medio de las plataformas y páginas web atención a los usuarios, donde es requisito, aportar datos personales, los cuales para continuar con el proceso se deben autorizar el manejo de la información, esto se realiza por medio de la autorización de tratamiento de datos personales, esta aceptación debe de ser voluntaria y consciente.

A partir del anterior planteamiento, se formula el siguiente interrogante: ¿De qué forma la Superintendencia de Industria y Comercio realiza un control sobre el uso adecuado, seguro y

limitado de los datos personales del usuario de entidades financieras y bancarias con respecto a la ley 1266 de 2008, en concordancia con la Ley 1581 de 2012? Para brindar la posible respuesta a esta pregunta, se abarcan 3 puntos esenciales:

- **Indicar las sanciones estipuladas en la Constitución Política de Colombia, respecto al incumplimiento de la normativa de protección de Habeas Data.**

En Colombia hay una entidad encargada de monitorear y regular el manejo de datos personales o Hábeas Data con base en la ley 1266 de 2008, que reza así “Habeas Data”, “*(...)por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (..)*” y dicha entidad es la Superintendencia de Industria y comercio, ente encargado de gestionar denuncias y sancionar empresas por el incumplimiento de la normatividad establecida con respecto a la protección de datos personales, referenciada en la ley 1581 de 2012.

De acuerdo a lo citado en las anteriores líneas, para mencionar un ejemplo, usualmente, en la actualidad, las redes sociales obtienen bastante información sobre sus usuarios, al punto que brindan estos datos a terceros, en este caso marcas y productos de distintas empresas que con este conocimiento obtenido establecen contacto con las personas para ofrecer sus servicios sin que estas les hayan proporcionado directamente información alguna.

A manera de ejemplificación, un artículo publicado en el año 2018 por el diario inglés The Guardian expone la manera en la que la firma Cambridge Analytica recopiló información de 50

millones de personas en 2014, esta información se recopiló por medio de la aplicación Facebook y contaba con cerca de 300.000 participantes, el escándalo reveló que los sucesos se ubicaron en un periodo de tiempo que coincidía con las campañas presidenciales de Estados Unidos, es decir que la información recopilada fue utilizada con intereses políticos. Este tipo de hechos refleja la sensibilidad que despiertan los datos hoy más que nunca en un mundo empresarial más competitivo.

En concordancia con estos casos mencionados surge la necesidad de establecer el siguiente punto a tratar:

- **Determinar las debilidades y fortalezas que tiene la Superintendencia de Industria y Comercio con respecto a salvaguardar los datos suministrados por los usuarios a través de redes sociales y plataformas digitales que suministran esta información a terceros con fines de marketing e intereses políticos.**

Matriz DOFA 2022:

MATRIZ DOFA 2022	
Debilidades	Oportunidades
<ul style="list-style-type: none"> <li>• Persistencia de procesos y controles manuales.</li> <li>• Dificultades para rotar el talento humano entre áreas, de acuerdo con las necesidades de los procesos.</li> <li>• Repesamiento de procesos de vigencias anteriores.</li> <li>• Bajo nivel de uso y apropiación de algunas herramientas tecnológicas.</li> <li>• Personal insuficiente para orientar el Sistema de Gestión Ambiental.</li> </ul>	<ul style="list-style-type: none"> <li>• Mejoras al marco normativo de la Entidad.</li> <li>• Avances en plan de vacunación contra el Covid-19 y reactivación económica.</li> <li>• Nuevas funciones asignadas a la Entidad en materia de supervisión a cámaras de comercio.</li> <li>• Permanente interacción con el sector privado.</li> <li>• Políticas de Estado orientadas a la automatización de trámites.</li> <li>• Regulación favorable en materia ambiental, de seguridad digital y de seguridad y salud en el trabajo.</li> <li>• Conciencia global sobre el cambio climático y la necesidad de proteger el medio ambiente.</li> </ul>
Fortalezas	Amenazas
<ul style="list-style-type: none"> <li>• Implementación de nuevos desarrollos tecnológicos en procesos de insolvencia.</li> <li>• Alto conocimiento técnico y experiencia .</li> <li>• Certificación de los procesos internos en calidad, ambiental y seguridad de la información.</li> <li>• Profesionales capaces y comprometidos.</li> <li>• Infraestructura física y tecnológica adecuadas.</li> <li>• Adopción de mejores prácticas y toma de conciencia en materia ambiental.</li> <li>• Certificación como Empresa Familiarmente Responsable.</li> <li>• Planta de cargos recién modernizada.</li> </ul>	<ul style="list-style-type: none"> <li>• Crisis de abastecimiento a nivel mundial que afecta a distintos sectores económicos.</li> <li>• Ataques cibernéticos a los sistemas informáticos de entidades estatales.</li> <li>• Coyuntura económica nacional marcada por un alto nivel de precios y devaluación del peso frente al dólar.</li> <li>• Malas prácticas empresariales.</li> <li>• Aparición de nuevas variantes del virus Covid-19.</li> </ul>

Al momento de indagar respecto a las debilidades y fortalezas que maneja la Superintendencia de Supersociedades, por ejemplo, la cual se encarga de brindar asesoramiento al Gobierno Nacional y hacer parte en el desarrollo de las políticas en todos los campos que tengan relación con la inspección, vigilancia y control de las sociedades comerciales y empresas unipersonales, la matriz DOFA 2022 que se muestra en la anterior ilustración, establece de manera gráfica, cuáles son las debilidades, fortalezas, amenazas y oportunidades a las que se enfrenta la entidad para el periodo en cuestión. Haciendo un análisis a este a comparación de años anteriores, como es 2018, se encuentra que presentan similitudes en ítems que figuran como fortalezas y debilidades, donde se refieren a aspectos como personal de planta, aspectos ambientales, la situación de la economía nacional e internacional, sin embargo, para el tema en cuestión se puede percibir cómo se incluye cada vez con mayor énfasis la implementación de la tecnología para los procesos de la entidad.

Matriz DOFA 2018:

MATRIZ DOFA 2018					
<b>FODA</b>		OPORTUNIDADES - O		AMENAZAS - A	
		O1.	Organismos internacionales que regulan el derecho societario	A1.	Incremento de procesos como consecuencia de la crisis económica que afecta a todos los sectores
		O2.	Interacción continua con el sector privado	A2.	Reforma legislativa en relación con las competencias de la superintendencia.
		O3.	Inclusión en el PND de acciones encaminadas a promover mayor productividad de determinados sectores económicos y delación de riesgos.	A3.	Reportes de organismos internacionales en cuya formación no participe la entidad.
		O4.	Políticas de Estado relacionadas con automatización de trámites	A4.	Riesgo de corrupción externo
		O5.	Regulación en materia de implementación y uso de las tecnologías de la información como apoyo a la gestión de las Entidades del Estado.	A5.	Fuga de información por hackers o intrusos en los sistemas de información de la Entidad
		O6.	Necesidad de medir el impacto del sistema en la economía	A6.	Costantes cambios en materia jurídica y contable
		O7.	Nueva regulación o reformas en materia de insolvencia, mercantil e inspección, vigilancia y control		
		O8.	Regulación internacional en materia de políticas de prevención y control en materia de riesgos como lavado de activos y financiación del terrorismo, riesgo operacional e inadversidad.		
		O9.	Crisis económica mundial que afecta todos los sectores económicos		
		O10.	Nuevas directrices de seguridad y salud en el trabajo		
		O11.	Regulación en materia de acceso a la información pública		
FORTALEZAS - F		Estrategias OFENSIVAS		Estrategias DEFENSIVAS	
F1.	Conocimiento técnico en el cumplimiento de las funciones	O6;O7;O9; F1	Elaboración de propuestas (proyectos decretos en materia de insolvencia o reglamentación para efectiva supervisión de sociedades)	F4;A3	Medición del impacto del sistema de insolvencia en la economía para identificar oportunidades de mejora en los indicadores internacionales que miden la eficacia del sistema
F2.	Mayor cobertura a nivel nacional a través de las intendencias regionales para atender los procesos	O6, O2, O8; O7;F4	Medición del impacto del sistema de insolvencia en la economía para identificar oportunidades de mejora en los indicadores internacionales que miden la eficacia del sistema	F2; A2	Desarrollar las funciones de la delegatura de manera oportuna, celeridad y con altas calidades técnicas.
F3.	Información disponible, oportuna, confiable y con calidad.	O1;O5;F5;F8;F7	Adoptar buenas prácticas que permitan el mejoramiento de los procesos y gestión de la Entidad	F3;A4	Coordinar la determinación de políticas y estándares en términos de estructura, registro, modificación y reporte de los datos utilizados, para garantizar que la información que se obtiene de ellos sea consistente y confiable.
F4.	Administración de la base de datos más completa en materia de insolvencia en el país	F8;O11	Fortalecer los canales de interacción con los usuarios con el fin de impactar de manera positiva el acceso a la información, trámites y servicios que presta la superintendencia.	F1;A2;A6	Proyectar reformas e iniciativas legislativas
F5.	Contar con arquitectura empresarial	F8;O10	Adecuar la infraestructura física para prestar un mejor servicio a nivel interno y externo	F7;A5	Proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la adecuada gestión de la seguridad de la información de los procesos
F6.	Adopción de mejores prácticas tecnológicas para la gestión de TI	F7;O10	Fortalecer el clima organizacional, mejorando la calidad de vida laboral con miras a incrementar la productividad de la organización.		
F7.	Implementación de estándares nacionales e internacionales para la gestión y seguridad de los procesos				
F8.	Infraestructura física adecuada				
DEBILIDADES - D		Estrategias REORIENTACIÓN		Estrategias SUPERVIVENCIA	
D1.	Planta de personal insuficiente para desarrollar Nuevas funciones otorgadas a la Entidad	O4;O5;O7; D1;D2;D4;D5	Gestionar y fortalecer las soluciones y servicios de TI para agilizar y controlar los procesos relacionados con las necesidades, atención de trámites y servicios prestados por la Entidad	D1;D2;D4; A1;A2;A4	Gestionar y fortalecer las soluciones y servicios de TI para agilizar y controlar los procesos relacionados con las necesidades, atención de trámites y servicios prestados por la Entidad
D2.	Controles manuales en el ejercicio de las funciones	O3;D3	Generar valor agregado a la información financiera reportada por los supervisados mediante un análisis de indicadores económicos y financieros, que permitan generar acciones de seguimiento y prevención de riesgo de los sectores productivos objeto de análisis.	D7;A3	Implementar soluciones tecnológicas que permitan consolidar, actualizar y disponer información para la toma de decisiones.
D3.	Dependencia de información y políticas emitidas por entes externos.	O4; D6	Adoptar mecanismos que agilicen la atención de las quejas presentadas por los diferentes grupos de interés que involucran sociedades supervisadas.		
D4.	Insuficiencia de recurso humano para atender incremento en volúmenes de solicitudes y procesos				
D5.	Vencimiento de radicaciones en algunos grupos				
D6.	Falta de herramientas para agilizar el desarrollo de los procesos en la delegatura.				
D7.	No contar con información de indicadores consolidada				

Así pues, las debilidades que se enuncian para el año 2022, refiriéndose a aspectos tecnológicos, consisten en que a pesar de que atravesamos una era digital, aún persisten los procesos y controles manuales en diferentes campos, además de que hay poco “uso y apropiación de herramientas tecnológicas”, en algunos sectores de desempeño laboral, dando a relucir la

inminente necesidad de automatizar los procesos lo máximo posible. Sin embargo, también se evidencia en las fortalezas expuestas, la implementación de desarrollos tecnológicos por parte de muchas empresas que además de esto, cuentan con infraestructura física y tecnológica adecuada. Esto denota, que hoy por hoy, la mayoría de las compañías que prestan algún servicio están a tono con la tecnología, la era digital, y que las que no lo están aún, tienden a acoplarse a este sistema. Por otro lado, respecto a las políticas de seguridad de la información y protección de datos personales menciona que la página web de la entidad cuenta con su respectivo certificado digital de sitio seguro, además, mencionan con el motivo principal de salvaguardar los datos personales de los usuarios se guían principalmente por la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, desarrollados posteriormente, y por su política de tratamiento de datos la cual está completamente basada en la ley y el decreto mencionados.

- **Identificar cuáles son los datos personales más comunes, que se almacenan en los formularios y plataformas digitales de las entidades bancarias y financieras, una vez aceptados los términos y condiciones.**

Para identificar efectivamente los tipos de datos personales, es esencial determinar el significado de “dato”, el cual proviene del latín “datum”. Refiriéndose a todo tipo de información ya sea de forma alfabética o numérica, específicamente para el caso en cuestión, o sea, la recopilación de información personal por parte de entidades financieras, estos datos privados se utilizan para individualizar a un sujeto con su información básica, siendo esta su nombre, edad, información de contacto y esencialmente en el término de la investigación, información financiera;

es por ello que ley 1266 de 2008 clasifica los datos “datos privados” “datos semiprivados” y “datos públicos”, también, la Ley 1581 de 2012 establece una clasificación especial de los datos personales, los titula “Datos sensibles” y “Datos personales de los niños, niñas y adolescentes”

La normatividad mencionada en el párrafo anterior, define el dato público los que por mandato de la ley o la constitución están definidos como la información que se encuentra contenida en documentos de carácter público, sentencias judiciales debidamente ejecutoriadas (que no estén sometidos a reserva) y la información referente al estado civil.

Ahora bien, es necesario hacer una distinción: por su parte, el dato semiprivado no tiene naturaleza íntima, reservada y tampoco pública, esto quiere decir que el conocimiento o divulgación de esta información puede interesar no sólo a su titular sino a cierto sector o a la sociedad en general. Un claro ejemplo de este tipo de información, es el financiero y crediticio de actividad comercial; se refiere a “dato privado” la información de carácter íntimo o reservado, es decir, que tiene relevancia únicamente para la persona titular de la misma. Por último, los datos de tipo sensible, tratan acerca de la información que puede afectar directamente la intimidad del titular, su uso indebido puede generar su discriminación.

Para aclarar un poco más el asunto, la categoría que se está desarrollando en el presente artículo, tiene que ver con el dato semiprivado, con respecto a este la Corte Constitucional ??????? establece que para el tratamiento, divulgación o acceso del dato semiprivado deben tener una limitante, puesto que requiere de una orden de autoridad judicial o administrativa, además se debe

utilizar netamente para los fines propios de sus funciones, sean estas datos financieros, historias crediticias, reporte en las centrales de riesgo.

## FUNDAMENTACIÓN TEÓRICA

Los estudios del tratamiento que se realiza a la información almacenada en las diferentes bases de datos de diversas empresas han sido enfocados principalmente en el área comercial y financiera, si bien con respecto a la información personal se han adoptado medidas de seguridad razonables para generar así un impedimento de la divulgación y destrucción no autorizada.

Para entrar en contexto, en la actualidad, el avance tecnológico ha traído como resultado que el manejo de la información sea más rápido y eficaz gracias a la globalización, permitiendo así que las personas puedan estar conectadas desde diversos lugares del mundo a través de laptops y teléfonos inteligentes, mediante el uso de internet. Pero en este artículo, cabe resaltar que, si bien los medios tecnológicos facilitan el manejo de datos personales por medio de entidades bancarias y financieras, se prestan para que se pueda dar un mal manejo de las mismas las cuales podrían generar diversas consecuencias para la población en sí.

En concordancia con lo anterior dicho, nace la necesidad de identificar la **importancia de contar con un Marco de Protección de Datos**. Para esto se debe mencionar que, para Unión Europea, la protección de datos se trata como un derecho fundamental, como mencionó Ralf Sauer. *“Esta consideración implica que el individuo debe tener control sobre sus datos y la obligación del Estado de proteger al individuo del riesgo de interferencia del gobierno en el uso de estos*

*datos, además del procesamiento de los mismos por parte de compañías.*” Según lo anterior este afirmado por la Organización de las naciones unidas, en su manual para parlamentos N° 26.

Como se ha reiterado en el presente artículo, como consecuencia del crecimiento exponencial de la revolución digital, las distintas entidades del sector financiero se han visto en la necesidad de acoplarse al uso de la tecnología, y precisamente uno de esos aspectos en los cuales han centrado su atención ha sido mediante la recolección de datos de sus clientes a través de formularios electrónicos, páginas web y aplicaciones, con el fin de expandir su campo de atención, evitando que sus usuarios por cualquier duda o solicitud se vean en la obligación de desplazarse hacia sus sucursales físicas. Es por eso que este sistema digital que se ha adoptado para ese tipo de trámites agiliza y optimiza el proceso. En consecuencia, el uso de información personal para dinamizar los procedimientos en diferentes ámbitos, también puede significar el uso indiscriminado de esa información para fines distintos. Un ejemplo reciente puede ser el caso de Cambridge Analytica. *“Este evento ha demostrado que el uso y abuso de la utilización de datos amenaza el funcionamiento de la democracia y la integridad de los procesos electorales”* menciona Ralf Sauer, jefe Adjunto de la Unidad de Flujos Transfronterizos y Protección de Datos de la Comisión Europea.

Casos como el anteriormente mencionado generan desconfianza con respecto a los usuarios que diariamente interactúan con las bases de datos que manejan las grandes empresas para dinamizar sus procedimientos, esto conlleva al entorpecimiento del progreso tecnológico y la oferta de mejores servicios públicos que deriven de este progreso.

Con base en lo mencionado anteriormente es importante resaltar las diferentes ventajas competitivas que conlleva la protección de datos, surgen entonces conceptos novedosos como el desarrollo de tecnologías de Inteligencia Artificial, Machine Learning y Ciencias de Datos, las cuales para su debido funcionamiento requieren de bases de datos bastante amplias. El experto europeo Sauer hace énfasis en la importancia de una adecuada política de protección de datos para el correcto funcionamiento y desarrollo de estas nuevas invenciones del hombre. *“En el ámbito económico, las compañías que trabajan con estas tecnologías muchas veces requieren intercambio de datos y la utilización de datos transfronterizos, por lo cual una buena legislación de protección de datos en el país de origen de estas empresas representa una fuerte ventaja competitiva.”* Precisamente esas ventajas competitivas consisten en que, si se endurecen las políticas de protección de datos, esto genera que las empresas más fuertes del mercado se esmeren por garantizar al usuario mayor seguridad y protección de sus datos personales.

Por otro lado, respecto a la esfera social, empieza a denotarse la relevancia de la protección de datos para la defensa de los diferentes intereses públicos tales como la reputación y el buen nombre de los clientes, información específica como sus lugares de residencia, empresas donde laboran, detalles de sus salarios, tipos de contrato laboral, bienes a su nombre, que pueden ser utilizados por terceros con fines de suplantación de identidad, fraude, estafa, difamación o robo, entre otros. Un claro ejemplo del incremento exponencial del uso de intercambio de datos de forma digital por parte del sector financiero respecto a sus clientes, se remonta al año 2020, donde la humanidad se enfrentó a la pandemia Covid-19, cada individuo pudo evidenciar como en todas las esferas se presentó un masivo intercambio de datos, tanto a nivel gubernamental, empresarial y personal.

En otro orden de ideas, la protección de datos es esencial para las empresas y autoridades públicas alrededor del mundo, pues esta está diseñada para prevenir posibles ataques de su seguridad y mitigar sus posibles efectos como, por ejemplo, sobornos, hurtos, difamación, para mencionar solo algunos. Otro tipo de posibles ataques, puede ser por medio de software malicioso “ransomware”, logrando que los delincuentes accedan a la información empresarial de alguna compañía la cual incluye propiedad intelectual o hasta secretos comerciales.

Además, el impacto global de la circulación de información constante genera la necesidad de implementar acuerdos internacionales que regulen o traten sobre la protección de datos personales, es por esto que Ralf Sauer menciona: *“En un mundo globalizado, en el que los datos se mueven con gran facilidad a través de las fronteras, es importante contar con un régimen sólido de transferencias internacionales de datos. No basta con detenerse en la frontera, ya que el tipo de protección que un gobierno puede garantizar en su país puede verse fácilmente socavado al trasladar los datos al exterior.”*

En el área del derecho comparado se desarrollan dos tipos de modelo de protección de datos, en primer lugar, el modelo centralizado, que se implementa principalmente en países europeos, su postulado principal es aplicar estándares generales para la protección de todos los datos, le deben aplicar exactamente los mismos principios, garantías y normas, sin embargo, estos son susceptibles de implementar estándares especiales sin que esto signifique derogar los estándares generales. Este modelo se caracteriza por contar con un ente de vigilancia central y autónomo que vele por el cumplimiento de los estándares normativos.

Por su parte, el modelo sectorial no está sometido a una misma regulación de los datos personales que recolecta, ya que se tiene en cuenta las diferentes características que presenten estos y de esta manera brindar cierta medida de poder de acceso e intervención a las autoridades, por ejemplo, con respecto a su privacidad, si posee cualidades de seguridad nacional, entre otros.

Para mencionar un ejemplo en América Latina, específicamente en Perú, se le otorga al habeas data un carácter constitucional bajo el título de “libertad informática”, tomando como referente al país alemán quien habla del “derecho a la autodeterminación informativa”. El Habeas Data en Perú cuenta con los siguientes objetivos principales: Acceso a la información, Actualización, rectificación, exclusión y reserva de la información.

Ahora bien, para dar un sucinto marco legal, de la manera en que se abarca el tema del habeas data en Colombia, es importante traer a colación una norma constitucional consignada en el artículo 15 de la Constitución Política de Colombia, la cual le otorga un significado importante al HABEAS DATA, mencionando “el derecho fundamental a la intimidad personal, familiar y al buen nombre”, obligando al estado a velar por estos aspectos de la vida de los ciudadanos.

En ese orden de ideas, a raíz de lo anteriormente mencionado, se han desarrollado diferentes normas de carácter legislativo, para llenar distintos vacíos que van surgiendo respecto al tema del manejo de datos a lo largo del tiempo en Colombia.

Al respecto de este tema que se viene mencionando, surgió la LEY 1273 DEL AÑO 2009 “*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones...*”. Sin embargo, para el presente año, surge la necesidad de implementar un tipo penal que regule los delitos que afecten la privacidad de datos, prestando especial atención al hecho de formar parte de los derechos constitucionales fundamentales.

En segundo lugar, de forma cronológica está el *DECRETO REGLAMENTARIO 1727 DE 2009* “*por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.*” Por medio del mencionado, regulan los estándares mínimos de información, donde las entidades financieras que cuenten con bancos de datos deben prestar especial atención, se divide en tres partes Información a nivel general del usuario titular de la información, Sector Financiero (productos y obligaciones adquiridos por el titular con diferentes entes que se someten al control y vigilancia de la Super Financiera) y Sector Real (obligaciones contraídas por el titular de la información con personas naturales o jurídicas diferentes a las enunciadas en el Sector Financiero)

Históricamente hablando, también se creó la *LEY 1581 DE 2012*, “*Por la cual se dictan disposiciones generales para la protección de datos personales.*” Su importancia radica en la regulación de derechos tales como habeas data y derecho a información. Establece qué datos son sensibles, la cual NO podrán ser divulgados, dichos datos son aquellos que afectan la intimidad del titular, datos relativos a la salud, vida sexual y los datos biométricos; Ahora, cuando se vaya a trasladar, cruzar información personal se deberá solicitar autorización previa e informada del titular y establecer a qué personas o entidades se les puede brindar la información.

El decreto reglamentario 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012” mediante este decreto se regulan diferentes aspectos de protección de datos, aclarando diferentes conceptos y desarrollando aspectos tales como son la recolección de datos, solicitud de autorización, modo de obtener y su revocatoria, entre otros.

El DECRETO REGLAMENTARIO 886 DE 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.” Mediante este se regula lo relacionado con Registro Nacional de Bases de Datos o por sus siglas (R.N.B.D), en este se establecen los requisitos mínimos que deberán cumplir las entidades financieras al momento de inscribir las bases de datos.

Ahora, a nivel jurisprudencial las sentencias más relevantes en el asunto son las siguientes:

**SENTENCIA T- 414 DE 1992:** Con Magistrado ponente el dr. Ciro Angarita Barón, se tutela el Derecho a la intimidad, a la libertad personal y a la dignidad, corte constitucional.

El caso mencionado, trata acerca de una acción constitucional de tutela que se interpone por un usuario que se encontraba reportado en una central de riesgo como deudor moroso del Banco de Bogotá, por lo que el accionante adquirió una obligación mediante pagaré en el año 1981. Mediante actuación judicial fue declarada prescrita en el año 1987, pese a la solicitud del ciudadano para ser retirado de la base de datos de deudores morosos no tiene éxito. En este caso, la corte desarrolla conceptos como el derecho a la información y la intimidad; el dato y su propiedad; las bases de datos y el derecho. Resalta de manera primordial la manera en que el derecho a la intimidad prima sobre el derecho a la información. Lo que se pretende con este caso citado, es demostrar que a medida que se han dado ciertas situaciones que vulneran los derechos de los ciudadanos por parte de las entidades financieras, es demostrar que gracias a los mismos se han evidenciado ciertos vacíos legales respecto a los cuales ha surgido la necesidad de una reglamentación por parte de los entes competentes del estado.

## **METODOLOGÍA**

Respecto a la metodología que se utilizó en la realización del artículo, se considera que es una investigación aplicada porque aborda un problema en específico y se pretende brindar una posible solución que aporte a la sociedad, en lo que concierne al hecho de evidenciar que no existan vacíos legales en materia de vigilancia y regulación, en cuanto al uso de la tecnología para el tratamiento de datos por parte de las entidades financieras, con el fin de garantizar que no se vulneren los derechos a los ciudadanos por un mal uso de su información personal suministrada a dichas entidades a través de formularios electrónicos, páginas web o aplicaciones. En este orden de ideas, el campo de acción en el cual se desarrolla la temática abordada, puede denominarse como sociojurídico, debido a que el propósito del mismo, se centra

fundamentalmente en el análisis sobre el cumplimiento y conocimiento por parte de la sociedad de las normas jurídicas, jurisprudencia y la todo lo relacionado al área de protección de datos. En este sentido, se busca examinar los estándares para la autorización y uso de los datos personales esto con base al Habeas Data. Además de ello, esta investigación también posee un enfoque descriptivo - cualitativo, en razón de la aplicabilidad que surge por parte de diversas entidades financieras, especialmente las bancarias, respecto a la ley de tratamiento de datos de los usuarios que al acceder a los servicios que ofrecen dichas entidades, aceptan la ley de tratamientos de datos, Habeas Data, desconociendo los peligros a los que están expuestos. Por esta razón este artículo está encaminado a analizar el cumplimiento en debida forma de los datos personales de los usuarios.

**RESULTADOS Y HALLAZGOS**

Ahora, frente al análisis de la matriz DOFA 2022 y 2018 de la Superintendencia de SuperSociedades, respecto a la implementación de la tecnología para los procesos de la entidad, se evidencian los siguientes hallazgos:

MATRIZ DOFA 2022	
Debilidades	Oportunidades
<ul style="list-style-type: none"> <li>•Persistencia de procesos y controles manuales.</li> <li>•Dificultades para rotar el talento humano entre áreas, de acuerdo con las necesidades de los procesos.</li> <li>•Represamiento de procesos de vigencias anteriores.</li> <li>•Bajo nivel de uso y apropiación de algunas herramientas tecnológicas.</li> <li>•Personal insuficiente para orientar el Sistema de Gestión Ambiental.</li> </ul>	<ul style="list-style-type: none"> <li>•Mejoras al marco normativo de la Entidad.</li> <li>•Avances en plan de vacunación contra el Covid-19 y reactivación económica.</li> <li>•Nuevas funciones asignadas a la Entidad en materia de supervisión a cámaras de comercio.</li> <li>•Permanente interacción con el sector privado.</li> <li>•Políticas de Estado orientadas a la automatización de trámites.</li> <li>•Regulación favorable en materia ambiental, de seguridad digital y de seguridad y salud en el trabajo.</li> <li>•Conciencia global sobre el cambio climático y la necesidad de proteger el medio ambiente.</li> </ul>
Fortalezas	Amenazas
<ul style="list-style-type: none"> <li>•Implementación de nuevos desarrollos tecnológicos en procesos de insolvencia.</li> <li>•Alto conocimiento técnico y experiencia .</li> <li>•Certificación de los procesos internos en calidad, ambiental y seguridad de la información.</li> <li>•Profesionales capaces y comprometidos.</li> <li>•Infraestructura física y tecnológica adecuadas.</li> <li>•Adopción de mejores prácticas y toma de conciencia en materia ambiental.</li> <li>•Certificación como Empresa Familiarmente Responsable.</li> <li>•Planta de cargos recién modernizada.</li> </ul>	<ul style="list-style-type: none"> <li>•Crisis de abastecimiento a nivel mundial que afecta a distintos sectores económicos.</li> <li>•Ataques cibernéticos a los sistemas informáticos de entidades estatales.</li> <li>•Coyuntura económica nacional marcada por un alto nivel de precios y devaluación del peso frente al dólar.</li> <li>•Malas prácticas empresariales.</li> <li>•Aparición de nuevas variantes del virus Covid-19.</li> </ul>

MATRIZ DOFA 2018

**FODA**

		OPORTUNIDADES - O		AMENAZAS - A	
		O1.	Organismos internacionales que regulan el derecho societario	A1.	Incremento de procesos como consecuencia de la crisis económica que afecta a todos los sectores
		O2.	Interacción continua con el sector privado	A2.	Reforma legislativa en relación con las competencias de la superintendencia.
		O3.	Inclusión en el PND de acciones encaminadas a promover mayor productividad de determinados sectores económicos y detección de riesgos.	A3	Reportes de organismos internacionales en cuya formación no participa la entidad.
		O4.	Políticas de Estado relacionada con automatización de trámites	A4	Riesgo de corrupción externo
		O5.	Regulación en materia de implementación y uso de las tecnologías de la información como apoyo a la gestión de las Entidades del Estado.	A5	Fuga de información por hackers o intrusos en los sistema de información de la Entidad
		O6.	Necesidad de medir el impacto del sistema en la economía	A6	Costantes cambios en materia jurídica y contable
		O7.	Nueva regulación o reformas en materia de insolvencia, mercantil e inspección, vigilancia y control		
		O8.	Regulación internacional en materia de políticas de prevención y control en materia de riesgos como lavado de activos y financiación el terrorismo, riesgo operacional e insolvencia.		
		O9	Crisis económica mundial que afecta todos los sectores económicos		
		O10	Nuevas directrices de seguridad y salud en el trabajo		
		O11	Regulación en materia de acceso a la información pública		
FORTALEZAS - F		Estrategias OFENSIVAS		Estrategias DEFENSIVAS	
F1.	Conocimiento técnico en el cumplimiento de las funciones	O6;O7;O9; F1	Elaboración de propuestas (proyectos decretos en materia de insolvencia o reglamentación para efectiva supervisión de sociedades)	F4;A3	Medición del impacto del sistema de insolvencia en la economía para identificar oportunidades de mejora en los indicadores internacionales que miden la eficacia del sistema
F2.	Mayor cobertura a nivel nacional a través de las intendencias regionales para atender los procesos	O6, O2, O8; F4	Medición del impacto del sistema de insolvencia en la economía para identificar oportunidades de mejora en los indicadores internacionales que miden la eficacia del sistema	F2; A2	Desarrollar las funciones de la delegatura de manera oportuna, celeré y con altas calidades técnicas.
F3.	Información disponible, oportuna, confiable y con calidad.	O1;O5;F5;F6;F7	Adoptar buenas practicas que permitan el mejoramiento de los procesos y gestión de la Entidad	F3;A4	Coordinar la determinación de políticas y estándares en términos de estructura, registro, modificación y reporte de los datos utilizados, para garantizar que la información que se obtiene de ellos sea consistente y confiable.
F4.	Administración de la base de datos más completa en materia de insolvencia en el país	F8;O11	Fortalecer los canales de interacción con los usuarios con el fin de impactar de manera positiva el acceso a la información, trámites y servicios que presta la superintendencia	F1;A2;A6	Proyectar reformas e iniciativas legislativas
F5.	Contar con arquitectura empresarial	F8;O10	Adecuar la infraestructura física para prestar un mejor servicio a nivel interno y externo	F7;A5	Proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la adecuada gestión de la seguridad de la información de los procesos
F6	Adopción de mejores practicas tecnologicas para la gestión de TI	F7;O10	Fortalecer el clima organizacional, mejorando la calidad de vida laboral con miras a incrementar la productividad de la organización.		
F7	Implementación de estándares nacionales e internacionales para la gestión y seguridad de los procesos				
F8	Infraestructura física adecuada				
DEBILIDADES - D		Estrategias REORIENTACIÓN		Estrategias SUPERVIVENCIA	
D1.	Planta de personal insuficiente para desarrollar Nuevas funciones otorgadas a la Entidad	O4;O5;O7; D1;D2;D4;D5	Gestionar y fortalecer las soluciones y servicios de TI para agilizar y controlar los procesos relacionados con las necesidades, atención de trámites y servicios prestados por la Entidad	D1;D2;D4; A1;A2;A4	Gestionar y fortalecer las soluciones y servicios de TI para agilizar y controlar los procesos relacionados con las necesidades, atención de trámites y servicios prestados por la Entidad
D2.	Controles manuales en el ejercicio de las funciones	O3;D3	Generar valor agregado a la información financiera reportada por los supervisados mediante un análisis de indicadores económicos y financieros, que permitan generar acciones de seguimiento y prevención de riesgo de los sectores productivos objeto de análisis.	D7;A3	Implementar soluciones tecnologicas que permitan consolidar, actualizar y disponer información para la toma de decisiones.
D3	Dependencia de información y políticas emitidas por entes externos.	O4; D6	Adoptar mecanismos que agilicen la atención de las quejas presentadas por los diferentes grupos de interés que involucran sociedades supervisadas		
D4	Insuficiencia de recurso humano para atender incremento en volúmenes de solicitudes y procesos				
D5	Vencimiento de radicaciones en algunos grupos				
D6	Falta de herramientas para agilizar el desarrollo de los procesos en la delegatura.				
D7	No contar con información de indicadores consolidada				

Comparando la matriz de 2018 con la actual, se puede percibir cómo se incluye la implementación de la tecnología para los procesos de la entidad, permitiendo que esta cuente con certificación de seguridad de la información. Aún así, las amenazas siguen siendo de la misma magnitud: ataques cibernéticos o fugas de información por hackers en los sistemas de información. En consecuencia, estas amenazas son posibles oportunidades de mejoramiento para la entidad, dando paso a regulaciones favorables de seguridad digital.

Las debilidades que se enuncian para el año 2022, refiriéndose a aspectos tecnológicos, consisten en que a pesar de que atravesamos una era digital, aún persisten los procesos y controles manuales en diferentes campos, además de que hay poco “uso y apropiación de herramientas tecnológicas”. Esto denota, que hoy por hoy, la mayoría de las compañías que prestan algún servicio están a tono con la tecnología, la era digital, y que las que no lo están aún, tienden a acoplarse a este sistema.

- **PROTECCIÓN DE DATOS PERSONALES**

Es importante precisar que cuando brinda autorización para el tratamiento de su información personal, se debe realizar con un fin específico, el cual deben informar de antemano a sus clientes. Sin embargo, si la información que brindó a la entidad es utilizada para fines distintos a los autorizados por el usuario, el debido proceso es acudir ante la Superintendencia, sin que una reclamación previa deba ser requisito.

De igual forma, en caso tal que la información brindada sea utilizada por personas no autorizadas, se puede, de igual manera, hacer valer el derecho de Hábeas Data ante la Delegatura de Protección de Datos Personales.

Las entidades financieras están en la obligación de salvaguardar la información suministrada por los usuarios a través de medios electrónicos, ya que estos datos personales pueden tener mal uso por parte de cibercriminales que buscan lucrarse por medio de identidades suplantadas, por ello es por lo que la seguridad de la información cobra vital importancia para la protección de la identidad de las personas y de sus cuentas bancarias.

Por lo tanto, el intercambio de datos personales entre personas naturales y jurídicas permite la interacción con otras empresas o entidades para que sea plenamente individualizada del resto de la sociedad, generando o dando espacio a diferentes flujos de información,

### **DIFUSION DE DATOS PERSONALES**

Si bien es cierto, el usuario al adquirir un producto con la entidad financiera, se somete a unos términos y condiciones que establece cada entidad basado en la norma, por lo que, es de gran importancia la lectura de la misma, un ejemplo muy claro es la difusión de datos a las centrales de riesgos, las cuales llevan el historial crediticio de cada persona con el fin registrar cada una de las obligaciones económicas adquiridas por las personas e identificar el estado en el cual se encuentran en el pago de sus obligaciones.

Ahora, cabe resaltar que en el código penal colombiano existe delito frente a la divulgación y/o difusión de datos personales mediante el ARTÍCULO 269F que se refiere a la VIOLACIÓN DE DATOS PERSONALES, casos en los cuales las entidades financieras filtran información personal sin autorización del usuario. En este tipo penal se castiga al sujeto que, sin estar facultado o sin autorización haga uso de códigos personales, datos personales contenidos en ficheros,

archivos, bases de datos o medios semejantes, con el fin de obtener provecho para sí mismo o para un tercero, puede incurrir en multa o prisión.

- **DERECHO AL BUEN NOMBRE:** Hace referencia principalmente a la manera en que la sociedad ve al individuo, esto en relación a su comportamiento en sociedad, siendo un derecho que puede ser vulnerado por un mal tratamiento de las entidades financieras a los datos personales de sus clientes.
- **SEGURIDAD DIGITAL FINANCIERA:** A nivel mundial se ha logrado evidenciar la necesidad de digitalizar los productos, esto en pro de la cuarta revolución industrial la cual se representa como la era digital en la cual se crea la necesidad de ofrecer productos de forma más rápida y eficiente por medios virtuales por ello las entidades bancarias se encuentran en la obligación de estar a la vanguardia y establecer todo los medios requeridos para satisfacer las necesidades de sus usuarios, por ende esto conlleva a que se brinde un seguridad digital financiera al almacenar datos de sus usuario, evitando así fraudes virtuales, suplantaciones y demás delitos informáticas.

Cabe resaltar que la importancia que toma la llamada “autodeterminación informática”, pues esta se trata de la facultad que recae en el sujeto al cual se refieren los datos, con el fin de autorizar su circulación, uso y conservación, y velar que se desarrolle conforme a las estipulaciones legales, sin embargo, al referirse a “libertad económica” se corre el riesgo de verse vulnerada al restringirse indebidamente derivada de la circulación de datos no veraces, o que no cuenten con la autorización del usuario titular o por la ley.” Esto podría generar daños

irreversibles a los clientes o usuarios en el ámbito moral, social y económico o incluso poner en riesgo su integridad personal.

En Colombia la entidad que se encarga de velar por la protección de los datos personales es la superintendencia de industria y comercio por lo anterior cabe mencionar que las sanciones aplicadas por incumplimiento de la normativa de la protección de datos personales se cumplen Conforme el ART 18 de la ley 1266 de 2008 de la siguiente manera:

*“La Superintendencia de Industria y Comercio y la Superintendencia Financiera podrán imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable, las siguientes sanciones:*

*Multas de carácter personal e institucional hasta por el equivalente a mil quinientos (1.500) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, por violación a la presente ley, normas que la reglamenten, así como por la inobservancia de las órdenes e instrucciones impartidas por dicha Superintendencia. Las multas aquí previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó.*

*Suspensión de las actividades del banco de datos, hasta por un término de seis (6) meses, cuando se estuviere llevando a cabo la administración de la información en violación grave de las condiciones y requisitos previstos en la presente ley, así como por la inobservancia de las órdenes e instrucciones impartidas por las Superintendencias mencionadas para corregir tales violaciones.*

*Cierre o clausura de operaciones del banco de datos cuando, una vez transcurrido el término de suspensión, no hubiere adecuado su operación técnica y logística, y sus normas y procedimientos*

*a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión. Cierre inmediato y definitivo de la operación de bancos de datos que administren datos prohibidos.”*

Es importante identificar los tipos de datos personales que se almacenan en los servicios bancarios y financieros, una vez aceptados los términos y condiciones. Los datos personales se clasifican en, Dato Público (determinado por la ley o Constitución Política como “todos aquellos que no sean semiprivados o privados.”); Dato Semiprivado (no cuenta con una naturaleza íntima, reservada, ni pública. su divulgación o conocimiento puede interesar no sólo a su titular sino a cierto sector o grupo de personas.); los Datos Privados (cuenta con una naturaleza íntima y reservada, tiene especial relevancia para su titular); por último los Datos Sensibles ( por su naturaleza de especial cuidado, su uso indebido puede afectar la intimidad del titular)

Esto quiere decir que las entidades bancarias recopilan datos semiprivados y datos sensibles, a continuación, se relaciona un ejemplo del uso de la información de los datos suministrados a un banco con el fin de adquirir un producto:

**Términos y condiciones**

**2. USO DE INFORMACIÓN:** Al presionar el botón "Solicitar", acepto y autorizo el envío de mis datos personales (tales como número de identificación, nombre y apellidos, correo electrónico, número de celular y/o teléfono fijo, monto, plazo y cuota simulada en caso de haber hecho simulación, ciudad de residencia) de manera expresa y voluntaria al Banco de Occidente o a quien represente sus derechos para que directamente o a través de terceros, el Banco de Occidente, su casa matriz, las filiales, subordinadas y/o asociadas del Banco, así como entidades aseguradoras y/o proveedores de asistencias con las que el Banco tenga convenios o acuerdos vigentes y en general las sociedades y demás Entidades vinculadas, o quien represente sus derechos, sea como beneficiario de estos derechos o en cualquier otro carácter puedan en cualquier tiempo acceder, almacenar, suministrar, reportar, procesar, divulgar, consultar, utilizar, computar, tratar y compartir, sea de forma verbal, escrita o a través de cualquier medio, mi información personal, de carácter comercial, financiero, crediticio y de servicios aquí consignada, la cual se recauda con fines comerciales, financieros, crediticios, operativos y de seguridad y con el fin de que se pueda brindar en la debida forma y con la adecuada diligencia información sobre los productos crediticios, financieros y comerciales del Banco de Occidente, en especial aquello correspondiente a los beneficios, ofertas, precios, tarifas, impuestos, estados de cuenta y todo aquello relacionado con los productos del Banco de Occidente, así como para que se puedan adelantar estudios de mercado, investigaciones comerciales y/o estadísticas, ofrecer de manera individual o conjunta con terceros, productos y servicios propios o de terceros, así como para ser notificado de noticias acerca de los cambios presentados en los productos del Banco de Occidente, con el objeto de conocer información crediticia, financiera y comercial de los productos y activos del Banco de Occidente y por tanto, la información aquí aportada tiene carácter crediticio, financiero o comercial. Igualmente, declaro que es de mi conocimiento que la información aquí consignada se tratará de acuerdo con los términos del Artículo 15 de la Ley 1266 de 2008 y sus modificaciones o adiciones que establecen lo siguiente:

"La información contenida en bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países podrá ser accedida por los usuarios únicamente con las siguientes finalidades:

- Como elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente
- Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas
- Para el adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulta pertinente.
- Para cualquier otra finalidad, diferente de las anteriores, respecto de la cual y en forma general o para cada caso particular se haya obtenido autorización por parte del titular de la información "

Mis derechos y mis obligaciones como titular de la información personal suministrada como usuario del PORTAL así como la permanencia de mi información en las bases de datos corresponden a lo determinado por el ordenamiento jurídico aplicable del cual, por ser de carácter público, estoy enterado.

Con base en todo lo expuesto en este artículo, La Superintendencia de Industria y Comercio evalúa anualmente indicadores de eficacia frente a las denuncias realizadas por la vulneración de los derechos a los que se hace mención en los artículos citados anteriormente.

Es menester, por lo tanto, en este contexto y panorama que se ha esbozado, la superintendencia de industria y Comercio tiene la facultad de sancionar conductas contrarias teniendo en cuenta la ley 1266 de 2008 en el art 19, que estipula un total de 6 los criterios para graduar las sanciones, siendo ejemplo de estos el beneficio económico, oponerse a la vigilancia de la Superintendencia de Industria y Comercio, el daño o peligro que genere al interés jurídico tutelado, entre otros.

## **CONCLUSIONES Y RECOMENDACIONES**

A modo de conclusión se encuentra que al referirse sobre el tema del derecho de hábeas data se hace mención de un derecho constitucional fundamental, plasmado en el artículo 15 de la Constitución Política de Colombia, que lo desarrolla como el derecho que poseen todos los ciudadanos a actualizar, conocer y rectificar la información que diariamente se recoge de ellas en las diferentes bases de datos y archivos de entidades privadas y públicas. Fundamentado en el artículo desarrollado se evidencia que Colombia cuenta con un marco normativo con cimientos fuertes con respecto a la regulación de la protección de los datos personales, la ley colombiana está fundamentada en el consentimiento expreso del titular de los datos. Respecto al tratamiento de datos que realizan las entidades financieras, es preciso mencionar que estas se encuentran reguladas y vigiladas por parte de la superintendencia de industria y comercio, la cual se encarga de brindar garantías al ciudadano respecto a la seguridad digital de su información personal.

## **RECOMENDACIONES:**

- A las entidades bancarias y a la Superintendencia de Industria y Comercio a utilizar los portales web, las redes sociales para sensibilizar a la gente frente a los derechos que se tienen respecto del habeas data.
- La implementación informática blockchain que permita verificar, validar, rastrear y almacenar todo tipo de información se encarga de prevenir la duplicación, brinda seguridad tanto a la entidad bancaria como al usuario.

## **REFERENCIAS BIBLIOGRÁFICAS**

- Superintendencia de Industria y comercio (2019), Preguntas Frecuentes, recuperado de URL <https://www.sic.gov.co/preguntas-frecuentes-pdp>
- Congreso de Colombia. (18 de octubre de 2012) Artículo 1,2 y 3 Título I. Ley Estatutaria 1581 de 2012
- Congreso de Colombia (31 de diciembre de 2008) Artículo 1 y 3. Ley Estatutaria 1266 de 2008
- Sánchez Acevedo, Torres Ávila, (2015). El derecho a la protección de datos personales y la responsabilidad de la administración pública en el tratamiento de datos personales, Editorial Universidad Católica de Colombia.
- Miguel Recio Gayo ( 2017) BIG DATA : hacia la protección de datos personales basada en una transparencia y responsabilidad aumentada pg. 5- 25
- Bertoni Eduardo (2012) Hacia una Internet libre de censura Propuestas para América Latina, Universidad de Palermo

- Salazar Edgar (2006) anuario NRO 29, EL HABEAS DATA EN EL DERECHO COMPARADO, Universidad de Carabobo.
- Iguarin Miguel, (2012) HABEAS DATA: DESARROLLO NORMATIVO Y JURISPRUDENCIAL EN COLOMBIA
- Sobre la protección de datos personales | Superintendencia de Industria y Comercio. Retrieved 21 June 2022, from <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>
- Sobre la protección de datos personales | Superintendencia de Industria y Comercio. Retrieved 21 June 2022, from <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>
- “Fuente: Superintendencia de Sociedades: [https://www.supersociedades.gov.co/nuestra\\_entidad/Planeacion/SitesPages/planeacionecuatrional.aspx](https://www.supersociedades.gov.co/nuestra_entidad/Planeacion/SitesPages/planeacionecuatrional.aspx)