# DATOS PERSONALES Y PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

JULIANA TEJADA BERRIO

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE DERECHO Y CIENICAS POLÍTICAS

FACULTAD DE DERECHO

MEDELLÍN

2021

# DATOS PERSONALES Y PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

JULIANA TEJADA BERRIO

Trabajo de grado para optar por el título de abogada

ASESORA

Mónica Patricia Aguilar Tobón

Abogada

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE DERECHO Y CIENICAS POLÍTICAS

FACULTAD DE DERECHO

MEDELLÍN

2021

**CONTENIDO**

Dedicado a mi familia: por su paciencia, soporte y fe.

## Resumen

El derecho a la intimidad, a la privacidad y la configuración del concepto de dato personal, ha implicado un despliegue jurídico en Colombia que ha pasado por pronunciamientos de las Cortes hasta su configuración en determinaciones legislativitas, teniendo una relevante consagración dentro de la Carta Política de 1991, pero cuyas formas tangibles y de aplicabilidad finalmente se ve reflejada en las leyes expedidas y su normatividad reglamentaria.

Los lineamientos establecidos por la norma no solo han delimitado los principios y el alcance de la protección de datos personales dentro de nuestro país, sino que han establecido de manera clara como las personas, tanto naturales como jurídicas, de carácter publico o privado, deben regir sus actos frente a los datos personales, dentro de lo preceptuado por la ley para su recolección, tratamiento y gestión, velando por la protección de los titulares y sus datos, con la posibilidad inclusive de ser sancionados si permiten la vulneración de los datos personales.

De esta forma, las organizaciones de carácter privado, como prestadoras de servicios y como tratantes de datos personales, deben garantizar durante todo el ciclo de vida del mismo su gestión y debida protección, aunando lo requerido por la ley y lo establecido en materia de seguridad de la información para la protección de datos a partir de preservación de confidencialidad, integridad y disponibilidad del dato.

Así, en el presente artículo no solo se realizará un esbozo del origen de la protección de datos personales y su normatividad dentro de Colombia, sino como dichos lineamientos jurídicos han exigido que las organizaciones privadas asuman responsabilidades que permitan proteger los datos personales, respondiendo a la normatividad, pero también a las exigencias de una sociedad cambiante y de proliferación en materia de tecnología.

**Palabras claves**: Datos Personales, Tipología, Protección de Datos Personales, Pilares de Seguridad de la Información, Confidencialidad, Integridad, Disponibilidad, Tecnología, Seguridad de la Información.

## Introducción

Dentro del presente artículo, y partiendo perfilamiento del derecho a la privacidad, intimidad y habeas data hasta llegar a la protección de datos personales, se llevará a cabo un análisis donde se identificará y establecerá como dentro de las organizaciones de carácter privado que recolecten y traten datos personales, se debe cumplir los lineamientos establecidos por la norma, ello en caminado a la salvaguarda de los derechos personales de sus titulares.

Así, se tiene como objetivo llevar a cabo un análisis en torno a la protección de datos personales, que, si bien tendrá como fundamento lo determinado por la norma, se planteará desde la ineludible conexión con la seguridad de la información y sus pilares: confidencialidad, integridad y disponibilidad.

En este entendido, se partirá de las necesidades y exigencias que surgen para el sector privado cuando requieren, captan, tratan y gestionan datos personales, especialmente en la diversificación de un mundo tecnológico que nos muestra una doble cara: agilidad en la recolección y tratamiento e incremento de amenazas sobre los datos personales, lo cual requiere la conservación de una serie de caracteres no solo de índole normativo sino desde la misma composición de la información, que deberá permitir evidenciar de forma expresa como se protegen los datos por parte del responsable.

Finalmente, se indagará y planteará la conexión entre la tipología del dato personal definida por la norma colombiana (público, semiprivado, privado y sensible), la finalidad del tratamiento de los datos y los pilares de la seguridad de la información, ítems que deberán ser componentes de un sistema de gestión y protección transversal de datos personales que no solo deberá responder a lo requerido por la norma si no por los cambios álgidos de la sociedad en sus diferentes ámbitos.

## 1. Protección de datos personales: aspectos generales

Los hombres entendidos desde su concepción existencial, se han caracterizado por la posesión de una serie de rasgos definitorios que han permitido individualizarlos, lo cual se ha traducido en una identidad, compuesta por diferentes atributos que han logrado caracterizar tanto sus rasgos intangibles (por ejemplo, el nombre) hasta sus particularidades físicas.

De ello se ha desprendido una serie de concepciones (filosóficas, históricas, antropológicas, científicas, jurídicas, etc.), que han generado diferentes marcos conceptuales definitorios y regulatorios, que no solo han propendido por la explicación e interpretación de dicha identidad, sino que se han dedicado a velar por su protección.

De tal forma, los hombres, tanto desde su individualidad como desde su pertenencia a una determinada comunidad o a un entorno social, a partir de la definición de su identidad hacen visibles una serie de atributos (que pueden ir desde su nombre hasta sus creencias), que le han permitido un reconocimiento como sujeto con particularidades y como individuo distinguible de otros, ello desprendido de su necesidad de reconocimiento y respeto por lo propio, tanto frente a sus pares como frente a diferentes figuras de poder.

Esta caracterización de identificación del ser humano y su necesidad de respeto y protección de la misma se traducen en lo que se ha denominado como intimidad, la cual irá evolucionando hasta llegar a un ámbito jurídico que ha logrado un tardío, pero necesario desarrollo de derechos que velan por la privacidad y protección del hombre en toda su concepción como ser individual, dotado de atributos y con una identidad determinada.

Si bien, en principio lo descrito anteriormente hace parte de una concepción primaria e inicial, son el punto de partida de todo un despliegue, arraigado e impulsado especialmente en materia jurídica, que no solo han dado pie al análisis sino a la

declaración de una serie preceptos que regulan y velan por su protección en diferentes ámbitos y territorios.

Así, desde lo básico y primitivo se da pie a la construcción de una concepción de identidad e intimidad (con elementos como el nombre y la propiedad), pero solo hasta la historia más reciente, específicamente durante el siglo XVIII, con el surgimiento de los denominados derechos humanos se eleva un reconocimiento tal a la identidad, el cual va más allá de la intimida para desglosarse en una serie de libertades cuya protección se vuelve primordial tanto en los territorios nacionales como dentro del ámbito internacional.

Todo ello, finalmente toma forma en una serie de mandatos tanto generales como particulares, que terminan propendiendo por el reconocimiento y protección de lo que hoy en día conocemos como datos personales, lo cual se erigió de manera contundente a partir de la Declaración Universal de Derechos Humanos de 1948, declaración en cuyo artículo 12 consagró: *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*[1]

De esta forma, se da inicio a un tema, cuya acogida comienza en mayor parte en países como Estados Unidos o dentro del territorio Europeo y de forma más tardía en Latinoamérica, tema que comienza a ser estudiado, tratado y consagrado en diferentes normatividades que velan por la protección de la identidad de los hombres y por la protección de sus datos, lo cual no ha resultado pacífico pues ha tenido que responder y tendrá que responder a las formas en las cuales avanza la sociedad, especialmente en un mundo donde impera el espectro tecnológico.

[1] https://www.un.org/es/universal-declaration-human-rights/

## 2. Protección de datos personales en Colombia

Si bien, podemos encontrar que el tema referido a datos personales tiene un génesis que vas más allá de consideraciones jurídicas y que ha evolucionado con el transcurrir de la historia y los cambios tanto individuales como sociales que han vivido los hombres, hasta consolidarse en una serie de declaraciones y legislaciones particulares de carácter obligatorio, dentro de Colombia podría hablarse de datos personales como un tema que data en décadas más recientes.

De tal forma, que solo para los años 90, con el surgimiento de una nueva Constitución Política dentro del escenario jurídico-político, se consagra de manera expresa en su articulado un derecho que propende por la protección de la intimidad y la data que caracteriza a una persona en su individualidad:

> ***ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen 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****.*
>
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*
>
> *La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.*[2]

Con la consagración de esta disposición se genera un marco protector sobre la intimidad y además se extiende a la protección de datos, el cual debe ser garantizado por el Estado y desde el Estado. A su vez, se concede el privilegio a las personas para la gestión de sus datos como titulares de los mismos frente a diferentes entes de carácter publico o privado que los hayan recolectado para un fin determinado. Concepción que da pie a un enfoque normativo dirigido al adecuado

[2] Subraya y negrilla del texto por fuera del texto original.

tratamiento de los datos de las personas, para evitar su perjuicio y para regular las acciones y sanciones en caso de concretarse alguna lesión sobre dichos datos.

Al respecto, es importante tener en cuenta que el tema dentro de nuestro ordenamiento comienza a ser tratado a partir de la acción que se ha denominado como habeas data, la cual ha sido entendida como

> *una garantía constitucional que permite a toda persona interesada acceder al conocimiento de los datos que consten de registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación. Esta información debe referirse a cuestiones relacionadas con la intimidad no pudiendo utilizarse por terceros sin derecho a hacerlo.* (Chanamé Orbe, 2003)

Concepto que inclusive ha tenido mención dentro de nuestra jurisprudencia, antes de su consagración normativa durante ley proclamada en 2008. Por ejemplo, a través de Sentencia T 414 de 1992, en la cual se señala el alcance, pretendido por el constituyente dentro de la creación de normas de normas, para la regulación y protección de la intimidad y la honra. Así, la Corte expresa

> *Como es bien sabido, cuando la doctrina se refiere a la intimidad bajo la forma de protección de la vida privada, lo hace tanto en un sentido amplio como en un sentido estricto.*
>
> *En el primero, la expresión designa todas las reglas jurídicas que tienen por objeto proteger la vida personal y familiar. Este es el alcance que le reconoce la Corte Europea de Derechos del Hombre al artículo 8o. de la Convención sobre la materia.*
>
> *En un sentido más estricto, la expresión se emplea también para designar exclusivamente un conjunto de normas que tiene por fin la protección de las personas contra atentados que afectan particularmente el secreto o la libertad de la vida privada.*

De esta forma, toma relevancia constitucional y jurídica la protección de datos de las personas como un derecho que emerge de su condición como tal, tanto en un

escenario de individualidad como social y que debe ser protegido de cualquier lesión o alteración. Generando de esta manera un derecho desglosado en acciones como: conocer, rectificar y actualizar los datos, entendiendo desde la norma de normas como puede tornarse un riesgo la recolección de información de un titular (tanto en la esfera pública como privada), lo cual terminaría repercutiendo en su intimidad y privacidad, por lo cual cualquier vulneración o posible vulneración debe ser evitada o sancionada.

En este sentido, la Corte Constitucional comenzó a incluir, describir y adoptar la protección de datos de los ciudadanos, como una materia de su competencia como órgano garante de derechos, por ejemplo, como lo hizo a través de la sentencia T 443 de 1994, en la cual advierte

> *El derecho al* ***habeas data*** *es un* ***derecho fundamental*** *concebido para contrarrestar los peligros del desarrollo de la informática que, junto con la electrónica y las telecomunicaciones, hace posible la difusión ilimitada de datos de la persona. El sistema centralizado de manejo de datos, con su creciente capacidad de recoger, almacenar, relacionar, transmitir información personal, familiar, comercial y de otra índole,* ***potencia los riesgos de manipulación de los datos…Este derecho otorga a la persona la posibilidad jurídica de impedir que terceras personas usen datos falsos, erróneos o reservados y desvirtúen así su identidad o abusen del derecho a informar****. El titular del derecho fundamental al habeas data goza del derecho a acceder al conocimiento de la información recogida sobre él en bancos de datos o archivos, controlar razonablemente su transmisión, limitar el período de tiempo en el que puede conservarse, definir los objetivos para los que puede ser utilizada, actualizar su vigencia o rectificar su contenido.* (Resalto en negrilla por fuera del texto original)

Si bien, es solo una muestra del análisis y entendimiento que venía adoptando nuestro ordenamiento sobre lo referido a datos personales, tanto desde su concepción como ser humano hasta todo lo que podría implicar su regulación desde el ámbito jurídico, comienza a ser notable su reconocimiento como derecho fundamental que requiere protección y transparencia frente a sus formas de

ejercicio, teniendo como conceptos de gran relevancia: información, voluntad, consentimiento, autorización, rectificación y actualización, todo ello conjugado dentro del ejercicio y validez de su derecho como titular de los datos.

Dado esto, se sientan bases de lo que más adelante se traduciría en normas que asientan dichas garantías básicas y fundamentales para la protección de información de sus titulares, no solo dentro de su identificación y captación sino dentro del tratamiento de la misma.

Ahora bien, entrada la década de los 2000 la Corte Constitucional continúa realizando pronunciamientos de gran importancia para el tema, por ejemplo, realiza el establecimiento de los principios sobre los cuales debe ceñirse este

> *Para la Corte, la especial necesidad de disponibilidad de información mediante la conformación de bases de datos personales, unida a la potencialidad de afectar los derechos fundamentales que apareja el desarrollo de dicha actividad, tornan indispensable someter el proceso de administración de los datos a ciertos principios jurídicos, con el fin de garantizar la armonía en el ejercicio de los derechos fundamentales de las administradoras, de los usuarios y de los titulares de los datos…*
>
> *…Para la Sala, reiterando la Jurisprudencia de la Corte, el proceso de administración de los datos personales se encuentra informado por los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad*. (Corte Constitucional, T-729, 2002)

Por tanto, con el magno propósito de garantizar un derecho fundamental, tal como el otorgado a los titulares de datos personales, todo lo relacionado con dichos datos, especialmente cuando están por fuera de la esfera privada de su titular, debe ceñirse a una serie de fundamentos base donde se vele por los datos desde su captura y dentro de todo su ciclo de vida en pro de la protección de la individualidad del ser humano.

Se trata entonces, de la proyección de un sistema de protección de datos personales, que debe tener en cuenta su clasificación y caracterización, que

vislumbra una protección con la capacidad de discernir en lo que se ha denominada e integrado dentro de nuestro ordenamiento como intimidad, buen nombre, y habeas data.

Resulta claro, como la Corte al proferir sus decisiones en el tema que nos ocupa, traza un camino jurídico que propende de manera evidente por la defensa de los ciudadanos, y no solo como ciudadanos, sino que parte desde su condición de ser, lo cual ha conllevado  a la consagración de derechos como el habeas data y a la información con un trasfondo sustancial que implica una protección proveniente tanto desde la espera publica como la privada, brindando particularidades, que inclusive, permiten distinciones tanto desde su concepción como derechos como desde su vulneración.

En esta perspectiva, la misma Corte nos esboza una distinción clara, en Sentencia T 017 de 2011, que permite hacer referencia a la protección de una individualidad de los ciudadanos que abarca su buen nombre, intimidad y acciones puntuales sobre su información

> *El artículo 15 Superior, consagra los derechos fundamentales al buen nombre y al habeas data, los cuales, de acuerdo con la jurisprudencia de la Corte, si bien guardan relación, tienen rasgos particulares que los singularizan, de tal suerte que la vulneración de alguno de ellos no siempre supone la violación del otro. Al respecto, esta Corporación ha escindido el núcleo de protección de tales derechos en los siguientes términos:*
>
> > *"Debe decirse que en lo relativo al manejo de la información, la protección del derecho al buen nombre se circunscribe a que dicha información sea cierta y veraz, esto es, que los datos contenidos en ella no sean falsos ni erróneos. Por su parte, la garantía del derecho a la intimidad hace referencia a que la información no toque aspectos que pertenecen al ámbito de privacidad mínimo que tiene la persona y que sólo a ella interesa. Finalmente, el derecho al habeas data salvaguarda lo relacionado con el conocimiento, actualización y rectificación de la información contenida en los mencionados bancos de datos" (Sentencia T-411 de 2005)*

En este orden de ideas, podríamos advertir el encuentro de un nutrido derrotero de pronunciamientos que desglosan a través de diferentes formas lo referido a derechos fundamentales como la intimidad, el buen nombre y el habeas data, todo ello finalmente como ante sala y desarrollo posterior de una consagración normativa más reciente, pero que marca un hito de gran consideración dentro de nuestro ordenamiento jurídico al regular como tal lo referido al habeas data: la ley 1266 de 2008.

Con la expedición de esta ley estatutaria, se establecen una serie de disposiciones a través de las cuales se regula el manejo de información cuyo contenido se encuentre en bases de datos tratadas dentro del sistema financiero, comercial, de servicios y crediticio, a la cual se añadieron dos decretos reglamentarios en 2009 y 2010: el Decreto 1727 y el Decreto 2952, respectivamente.

Posteriormente, durante 2012 es promulgada la ley 1581, ley de carácter estatutario, cuyo objeto se dirige a la protección de datos personales, con ella el espectro de la protección de datos anclado al tema de servicios, financiero y crediticio se amplía y nuestro país comienza a contar con una ordenación general y, a su vez, integra que propende por la protección de datos personal y su tratamiento, cobijando así derecho a la información, a la intimidad y reforzando las acciones otorgadas frente a esos derechos tales como conocer, actualizar y rectificar la información recogida de su titular.  Lay ley 1581 trae consigo la regulación de tres aspectos determinantes: 1. Requerimiento de la autorización del titular para la captación de sus datos 2. Políticas de Tratamiento que deben ser emitidas por responsables y encargados 3. Ejercicio expreso de los derechos de los titulares de los datos personales. (Rojas Bejarano, M, 2014)

Tanto la ley 1266 de 2008, como la ley 1581 de 2012, traen definiciones sustanciales no solo para la protección de datos personales sino para el

entendimiento de los mismos. Por su parte dentro de la ley 1266 de 2008 en su artículo 3, literal e), encontramos que se definen a los datos personales como

> *Cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados*.

Adicionalmente, nos entrega 3 tipos en los cuales pueden ser clasificados los datos personales: dato público (artículo 3, literal f), dato semiprivado (articulo 3, literal g) y dato privado (artículo 3, literal h), catálogo de tipos de datos personales que es complementado con la categoría de datos sensibles descritos dentro del artículo 5 de la ley 1582 de 2012.

De igual manera, tanto la ley 1266 como la 1581 traen consigo la determinación de un ente especifico de protección y vigilancia para la protección de datos personales: la Super Intendencia de Industria y Comercio (SIC). Por su parte la ley 1266 de 2008 acoge a dicha entidad como garante en su artículo 17: FUNCIÓN DE VIGILANCIA y la ley 1581 de 2012 lo hace a través de los estipulado en su artículo 19: AUTORIDAD DE PROTECCIÓN DE DATOS. Al respecto, debemos tener en cuenta que la designación de la SIC con dichas funciones ha permitido que dicha entidad realice pronunciamientos necesarios que han permitido dar claridad a la ley tanto desde su conceptualización, como desde su implementación.

De esta forma vemos un panorama normativo, que, aunque pueda tener vacíos y que debe adaptarse a los usos y nuevas formas que exige de la sociedad, nos permite afirmar que dentro de nuestro país se cuenta con normatividad que

apuntan al establecimiento de un sistema integral para el tratamiento de datos personales (tanto dentro del ámbito público como del privado), en el cual es clara la responsabilidad de protección por parte de aquellos que capturen y traten dichos datos, procurando en todo caso por la garantía del ejercicio de los derechos de los titulares, los cuales solo deben ser usados para las finalidades expresamente indicadas al titular para su recolección y almacenamiento.

Si bien, se podría describir un amplio derrotero de lo que regula la normatividad en Colombia en lo referido a datos personales, en definitiva, la inclusión de la principialistica es una gran victoria, pues no solo se queda dentro de un marco jurisprudencial, sino que se apunta a una protección real, palpable y efectiva de los derechos fundamentales en materia de datos personales (información, buen nombre, habeas data, intimidad), lo cual determina la administración de los mismos, para generar un equilibrio entre quienes recolectan y usan bases de datos con datos personales y los titulares de estos.

Así, de manera expresa dentro de la ley 1266 de 2008 (artículo 4) y dentro de la ley 1581 de 2012 (Título II, artículo 4) se consignan los principios rectores a los cuales deberá sujetarse la interpretación y aplicación de la ley en el marco del tratamiento de información y datos personales. Estos principios, finalmente, a pesar de que puedan revestir un alcance diferente, entran a regir como los pilares que guían los contenidos y ejercicio de la normatividad promulgada.

De tal forma que, la legalidad, la finalidad, la libertad, la veracidad, la transparencia, el acceso y circulación restringida, la seguridad, la confidencialidad, la temporalidad de la información y una interpretación integra de los derechos otorgados por la carta política se erigen como los lineamientos marco bajo los cuales debe trazarse la aplicación de la ley, su interpretación y la protección que deben recibir los ciudadanos dentro de su esfera privada y los datos personales que lo dotan de individualidad.

## 3. Pilares de seguridad de la información: confidencialidad, integridad y disponibilidad

No podemos desconocer que el tema referido a datos personales y todo lo que ello implica (recolección, tratamiento, almacenamiento, modificación, revocatoria, etc.) ha implicado el establecimiento de regulaciones, normativas, directrices y demás lineamientos de carácter jurídico, ello evidenciado tanto en Colombia como en el mundo.

Pero ello no ha determinado exigencias provenientes solo desde el marco jurídico, sino que ha impactado otros ámbitos, especialmente en materia privada y comercial, ello con el fin de tratar y proteger dichos datos, lo cual ha implicado retos, adaptaciones y determinaciones de carácter técnico que han desarrollado lineamientos que apuntan a la protección de los datos y de la información, y los cuales deben ir de la mano con lo decretado por la norma.

Por consiguiente, nos encontramos con estrategias de seguridad, establecidas partiendo desde análisis y elementos técnicos, que han dado vida a criterios que deben ser adoptados por entidades (públicas o privadas) con el fin de proteger y mitigar posible vulneración de la información que recolectan y tratan (esto para todo tipo de información, dentro de la cual se incluyen los datos personales). De allí se deriva lo que hoy en día conocemos como seguridad de la información y pilares de la seguridad de la información.

Al respecto, es importante realizar la siguiente precisión: no podemos partir del asumir como conceptos similares la seguridad informática y la seguridad de la información, pues si bien ambos son de gran importancia en un mundo en donde abunda el flujo de datos, entendemos que el objetivo principal de la **seguridad informática** es *mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable* Macías Valencia, D- Quiroz Zambrano, S. (2017)*.,* mientras que la

**seguridad de la información** hace referencia a el *conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información.* Calderón Alateco, L. (2015). Siendo la confidencialidad, integridad y disponibilidad los pilares que deben ser protegidos pues garantizan las dimensiones de la información.

Partiendo de la claridad conceptual realizada en líneas anteriores y para generar un marco que permita conectar lo referido a la clasificación de datos personales con los pilares de seguridad de la información (confidencialidad, disponibilidad e integridad) es necesario clarificar que se entiende por dichos pilares, en términos del Incibe-Instituto Nacional de Ciberseguridad

> *La **integridad** de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores.*
>
> *La **disponibilidad** de la información hace referencia a que la información esté accesible cuando la necesitemos.*
>
> *La **confidencialidad** implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.*

De esta forma se traza un marco claro en materia de seguridad de la información (en general incluyendo tanto aquella en la que se traten o no datos personales), cuya aplicabilidad debe partir de la identificación de información que se ha denominado como activos, es decir, información tan valiosa al interior de una organización que de la misma dependen la consecución de sus objetivos, en donde a partir de dicha identificación se establecen los lineamientos y medias necesarias para su protección.

Así, la determinación de las medidas de protección de la información estará asociada a diferentes factores, pero será fundamental partir de la identificación de la misma, estableciendo la menor o mayor importancia que tenga está dentro de los procesos y objetivos de una organización. Ello unido a la exigencia de un proceso

de adaptación acelerado que tenga la capacidad de responder a un mundo donde se trata la información a partir de elementos tecnológicos e intangibles.

Hasta este punto, encontramos como la información, y especialmente la que hace referencia a datos personales y la cual es tratada dentro de las organizaciones y cuya naturaleza determina su manejo, es un elemento de valor y no solo en cuanto a importancia operacional sino también económica, que hace que los entes que recolectan y tratan información de carácter confidencial y privada deban responder de manera permanente y visible ante las posibles pérdidas, vulneraciones o deteriores que puedan causar daño sobre los datos personales tratados sea de forma física o electrónica, teniendo especial relevancia aquellos que se encuentran dentro del espectro tecnológico.

Este panorama, ha creado peligros sobre la información, especialmente sobre los datos personales de sus titulares, en donde si bien los avances tecnológicos y el uso de las nuevas tecnologías han generado espacios de agilización y progreso, también han creado una fuente de peligro que se deriva desde la vulneración, evidenciada principalmente en los accesos no autorizados y en la lesión a la integridad, disponibilidad y confidencialidad de los datos.

Estas amenazas pueden concretarse y causar grandes vulneraciones sobre los datos personales y terminan traduciéndose en una afectación a los ya mencionados pilares de seguridad de la información (integridad, disponibilidad, confidencialidad), pues los datos personales pueden ser alterados y no conservar su completitud, podrían no estar disponibles cuando son requeridos o podrían ser accedidos por aquellos que no tienen autorización para accederlos, conocerlos, almacenarlos, tratarlos o disponer de los mismos. Es por ello que la identificación de estos pilares de cara a los datos personales son la forma previa requerida para establecer las estrategias de protección necesarias que permitan salvaguardar su integridad, disponibilidad y confidencialidad.

Teniendo en cuenta lo descrito anteriormente, podrán existir otros mecanismos con los cuales se gestione la información desde diferentes campos y entidades, involucrando diferentes elementos que incluyen la innovación y apuntan al desarrollo de acciones agiles y útiles, pero ello no queda a la deriva en un mundo en el cual nos enfrentamos a distintas formas de vulneración de información, por lo cual todas las herramientas referenciadas, las existentes y aquellas por existir deben estar sujetas a una serie de parámetros de seguridad (ya descritos como pilares) que permitan conservar un elemento innegociable de la información y sus datos personales: el acceso autorizado a ellos, su integridad y la disponibilidad tanto para sus titulares como para quienes los tratan.

Si bien, estos pilares como tal no han sido consignados de manera expresa dentro de una norma, por lo menos al interior de la legislación colombiana, si han sido acogidos dentro de parámetros unificados, que aunque no sean de obligatorio y generalizado cumplimiento, si se han convertido en estándares exigidos para garantizar la protección y resguardo de la información, especialmente dentro del ámbito empresarial y comercial, esto a través de la adopción y aplicación de ciertas normatividades como la ISO27001, la adopción de certificaciones como PCI DSS en el caso del escenario de las Tarjetas de Pago o la realización de auditorías, por ejemplo.

Lo anterior dirigido a salvaguardar la confidencialidad, integridad y disponibilidad de la información, lo cual genera confianza y respaldo a las compañías y en el escenario digital, pues la información debe ser protegida de manera tal que no pueda tener conocimiento de ella cualquier persona o entidad no autorizada, evitando su alteración y permitiendo que se encuentre completa, cuya modificación necesariamente requiere autorización además de garantizar el acceso a la misma.

De esta manera la seguridad de la información entra a tomar un papel protagónico en materia de manejo de la información, partiendo desde la protección de infraestructura física hasta el establecimiento de políticas, manuales,

procedimientos, metodologías y controles que incluyen elementos técnicos pero que tiene en cuenta el factor humano.

Así, lo que se ha denominado como nuevas tecnologías, ha implicado una interacción social entre entidades (de orden público o privado) y los titulares de datos personales a partir de la agilidad, abreviación y seguridad dentro de las diferentes prácticas y alcances a la hora de recoger y tratar datos personales, siendo requerimiento ineludible para regular el tema, lo cual ha sido tenido en cuenta y debe ser tenido en cuenta por los diferentes Estados. Lo anterior, de la mano con el entendimiento sobre la seguridad de la información y la seguridad informática, pues de ellas se deriva un poder ineludible, pero si regulable, que ha logrado suprimir barreras territoriales, espaciales y temporales para la recolección y circulación de datos personales, lo cual incrementa las exigencias de protección tanto de cara a las legislaciones como desde las configuraciones técnicas. (García Gonzales, A, 2007)

Teniendo en cuenta lo descrito, en efecto, las formas de manejar y gestionar la información actualmente implican necesariamente la implementación de elementos tecnológicos, donde ello no solo recae el peso de la gestión de datos sobre los elementos técnicos, sino donde debe darse una integración de factores humanos e inclusive de elementos éticos que no solo permitan promover y garantizar una recolección, almacenamiento y circulación segura de la información sino conservar la integridad y confidencialidad los datos, especialmente de los personales.

## 4. Protección de datos personales y pilares de seguridad de la información dentro de una entidad privada

En suma, con lo descrito en los capítulos anteriores hemos logrado esbozar un marco legal y desde la seguridad de la información, para la regulación y protección de la información, especialmente de datos personales dentro de Colombia, en donde el tema referido a la regulación de información de los ciudadanos y sus datos

personales ha tenido un recorrido que ha generado no solo pronunciamientos sino una definición normativa expresa, lo cual ha causado un impacto no solo de cara a la responsabilidad del Estado y sus entes sino dentro del ámbito privado, enfáticamente dentro de las empresas que capturan y tratan datos de sus titulares

Para realizar un anclaje entre lo referido a protección de datos personales y las consideraciones que se han establecido en materia de seguridad de la información a nivel de las diferentes entidades, especialmente las privadas y de carácter financiero, que nos permita realizar un análisis de la conexión, interacción y desarrollo de ambos temas dentro de las entidades privadas, se identifica la necesidad de partir de una claridad en términos jurídicos y es ¿cuáles son los tipos de datos personales a proteger?

De esta forma,

> *Se establece la existencia de información pública, semiprivada, privada y reservada. La* ***información pública*** *es aquella que puede obtenerse sin reserva alguna, entre ella los documentos públicos, habida cuenta del mandato previsto en el artículo 74 de la Constitución Política y de idéntico alcance en el artículo 323 del decreto 1377/2013.*
>
> *La* ***información semiprivada*** *es aquel dato personal o impersonal que, al no pertenecer a la categoría de información pública, sí requiere de algún grado de limitación para su acceso, incorporación a bases de datos y divulgación. Se trata de información a la que solo puede accederse por orden de autoridad judicial o administrativa y para los fines propios de sus funciones, o a través del cumplimiento de los principios de administración de datos personales antes analizados.*
>
> *Para la Corte, la* ***información privada*** *es aquella que se encuentra en el ámbito propio del sujeto concernido y, por ende, solo puede accederse a ella por orden de autoridad judicial competente y en ejercicio de sus funciones.*
>
> *Por su parte, la* ***información reservada*** *es aquella que solo interesa a su titular en razón a que se relaciona estrechamente con la protección de sus derechos a la dignidad humana, la intimidad y la libertad* (Subaraya en negrilla por fuera del texto original) Monsalve Caballero, Vladimir (2016)

Y si bien en nuestra legislación no existe una única ley que abarque su tipología, si se ha abordado por separado en diferentes pronunciamientos y se ha dejado por sentada dicha clasificación en diferentes leyes ya enunciadas, encontrando entonces datos personales de tipo público, semiprivado, privado y sensible. Tipos que se han determinado a partir de la determinación de la individualidad de un titular con dichos datos, y como dichos datos causan mayor o menor vulneración de las personas, cuando son expuestos.

De tal manera que, para determinar mecanismos de protección de datos personales al interior de una organización, es necesario entender su clasificación, pues esto se convierte en un filtro que permite generar trazabilidad durante el ciclo de vida del dato y además establecer las formas en que deben protegerse según su grado de divulgación.

En este punto es importante entender que al interior de cualquier organización que recopile datos personales de sus titulares se presenta un fenómeno en el cual se agrupan gran cantidad de datos personales de diversa índole por lo cual su tratamiento y protección debe estar en sinergia con los pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad, entendiendo que estos tres atributos deberán garantizarse en mayor o menor medida dependiendo si se trata de un dato personal público, semiprivado, privado o sensible.

Así, la clasificación de datos personales permite entender su concepción dentro del ordenamiento jurídico para a partir de ello poder realizar una labor organizativa en la cual se alineen las diferentes áreas, especialmente la jurídica y la de seguridad en la información, con el fin de generar estrategias efectivas de protección y mitigación de riesgos frente a las vulnerabilidades que podrían generarse frente al tratamiento de datos personales capturados. Se trata entonces de generar una estrategia que permita aplicar las directrices normativas en conjunto con las exigencias de seguridad y tecnología que encontramos latentes dentro del mundo corporativo.

En consecuencia, la protección de datos personales se ha convertido en un tema con alta sensibilidad en los últimos tiempos, especialmente gracias a la masificación de su recolección con diferentes finalidades y al innegable papel de la tecnología en su recolección, almacenamiento y protección. Así, el tratamiento de los datos personales ha implicado la asunción de una serie de responsabilidades, que a la luz de nuestra legislación requieren una demostración de la adopción de políticas, manuales, medios eficaces de atención y en sí la implementación de mecanismos de protección sobre estos datos.

Este panorama descrito ha venido regulándose desde la normatividad, tal como sucede en Colombia, pero debido a su magnitud ha requerido una visión holística que va más allá de un presupuesto jurídico y necesariamente integra otros ámbitos del conocimiento tal como el tecnológico, pues desde este último se han generado las formas y medios para recolectar, almacenar y tratar los datos personales.

De esta forma se ha creado una sinergia que necesariamente ha conllevado a exigir la adaptación entre los parámetros legales y los componentes tecnológicos creados y atados al tema de protección de datos personales, lo cual no resulta tareas fácil debido a la multiplicidad de conceptos y variables que rige cada área de conocimiento, no obstante, donde se hace necesario e indispensable velar por la aplicación de los avances tecnológicos en materia de tratamiento de datos pero garantizando de manera innegociable la protección de los datos personales de sus respectivos titulares.

De esta manera, es necesario partir de una consideración normativa en la cual por un lado se establece la definición del dato personal y por el otro la clasificación tipología del mismo (público, semiprivado, privado, sensible). Esto debe convertirse en la base para orientar todo lo referido a la protección de estos, pues una vez ser abordado con claridad al interior de cualquier organización o persona natural que recopile datos, se pueden e implementar una serie de medidas que propugnen por una protección concreta, eficaz y especialmente demostrado de los datos

personales. Así, este último concepto, que ha sido denominado como “responsabilidad demostrada”, será el que permita generar el lazo entre el marco jurídico referido a protección de datos personales y los parámetros de protección de la información.

Con lo anterior se parte del entendimiento de una base jurídica que requiere de acciones concretas, demostrables y palpables que demuestren el cómo frente a la protección de datos personales se realizan acciones que permiten conservar la privacidad del dato tanto de cara a su almacenamiento y tratamiento como de cara al titular y lo que el dato representa para este.

Es por ello que las entidades privadas, que, como prestadoras de diferentes servicios, para realizar y consolidar ofrecimientos y experiencias a sus usuarios, requieren la captura de información, especialmente de datos personales, con el uso de diferentes e mecanismos de innovación que necesariamente deben tener medidas y lineamientos que apunten no solo a la gestión sino protección de dichos datos.

Como resultado, las entidades de carácter privado, para el despliegue de sus portafolios, conciben como un intangible fundamental para el desarrollo y sostenimiento de sus operaciones: la información, los datos personales, lo cual les ha exigido la implementación de una serie de formas que no solo permiten su manejo y almacenamiento, sino que se encuentran dirigidos a procurar por su seguridad, generar modelos de riesgo, prevenir y tratar aquellos casos en los que se presenten los mismos.

Por supuesto, ello ha implicado la reevaluación, adopción y despliegue de estrategias de seguridad que apunten a proteger los datos en todas sus dimensiones, partiendo desde las concepciones y lineamientos legales hasta todo el despliegue en sitio y digital que implica la captura, circulación y flujo de la información.

Para ello es necesario que al interior de cualquier organización se vele por la preservación de la confidencialidad, integridad y disponibilidad de la información, pues sobre estas tres dimensiones se llevará a cabo la aplicación de las estrategias de protección que se vayan a determinar. Esto nos lleva a las siguientes cuestiones: ¿Cómo preservar la confidencialidad de los datos personales? ¿Cualquiera puede acceder a los mismos? ¿Qué pasa si los datos personales recopilados por una organización privada son alterados y no reflejan la realidad? ¿Cuáles serían las consecuencias de que dichos datos personales no estén disponibles para su titular al ser requeridos? ¿Cómo responder a estas situaciones sin quebrantar la norma?

Y para responder a estas y a otra multiplicidad de inquietudes que podrían presentarse, debemos entender que los datos personales son configurados como activos de información al interior de las organizaciones privadas, entendiendo como activo de información aquellos *conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados.* Figueroa Suarez, J- Rodríguez Andrade, R- Bone Obando- C, Saltos Gómez, J (2017).

Este entendimiento sobre los datos personales, partiendo desde la definición normativa de los mismos, implican una valoración, seguimiento y protección que apunte a la salvaguarda de todas sus dimensiones (confidencialidad, integridad y disponibilidad)

> *La evaluación de los activos de información de la organización en relación a estas tres dimensiones de la seguridad determina la dirección a seguir en la implantación y selección de medidas, también denominadas controles o salvaguardas. También debemos tener en cuenta que la adopción de un determinado control para mejorar la seguridad en una dimensión, puede afectar de forma negativa o positiva a otra de las dimensiones, por ello, es esencial conocer cuál de estas dimensiones es más importante proteger en cada sistema de información.* (Incibe- Instituto Nacional de Ciberseguridad. Protección de la información)

Por ello, dentro del sector privado debe partirse de la realización de una identificación normativa, en nuestro orden nacional a partir de lo determinado por las leyes 1266 de 2008 y 1581 de 2021 y todas sus normas reglamentarias, generando depuraciones de lineamientos particulares que hayan sido emitidos en materia de datos personales.

Con esto depurado proceder a la conformación de equipos de cumplimiento y a la generación de documentos marco que no solo integren los principios generales establecidos por la normas, sino que permitan un desglose táctico y estratégico que pueda verse reflejado dentro de la operatividad de cada organización, para la definición de un sistema de gobierno transversal que permita regular y atender todo lo relacionado con los datos personales: desde su recolección hasta sus posibles vulneraciones o depuración.

Este sistema de gestión sobre los datos personales no radica únicamente en cabeza del área jurídica o de cumplimiento dentro de una organización privada, todo lo que implique la protección de dichos datos debe involucrar diferentes áreas, tal como lo hemos expresado, la de seguridad de la información, pues solo con una visión y un ejercicio holístico de la protección de datos logrará identificarse el impacto, las necesidades y las medidas requeridas que permitan velar por los usuarios y sus datos.

Al respecto, con el fin de velar por la seguridad de los datos personales, es indispensable tener de manera visible el ciclo de vida de los mismos, para realizar un seguimiento desde su captura, pasando por su almacenamiento, finalidades, protección, gestión y depuración, ello a partir de la determinación de actividades articuladas con cabezas responsables visibles que involucren las distintas áreas.

De manera que la determinación de las medidas necesarias para lograr la protección de los datos personales implicará la fijación de los siguientes aspectos:

- *Determinar la importancia de la información que manejamos. El sector de negocio puede afectar a la naturaleza de la información que tratamos, en*

*particular en lo relativo a la privacidad de los datos personales de nuestros usuarios y por la existencia de información confidencial, cuya pérdida o deterioro pueda causar graves daños económicos o de imagen a la empresa.*

- *Identificar, clasificar y valorar la información según las dimensiones de seguridad son los pasos previos que van a dirigir la selección de las salvaguardas. Así, algunos activos de información serán muy confidenciales (estrategias, contraseñas, …), mientras que otros, como la página web o la tienda online, no podremos permitir que no estén disponibles.*
- *Tendremos también que conocer la naturaleza de los controles que podemos implantar. No sólo tendremos que considerar medidas técnicas como la instalación de un cortafuegos, sino que consideraremos también medidas organizativas, por ejemplo, implantar un plan de formación, establecer responsables de los activos o adaptarnos para cumplir con la legislación.* (Incibe- Instituto Nacional de Ciberseguridad. Protección de la información)

De ahí, que conservar la confidencialidad, integridad y disponibilidad de los datos personales debe ser una tarea que parta desde el enfoque de riesgos, donde se propone en este escrito, tener como norte lo que la norma ha denominado **finalidades**, pues a partir de la los objetivos y fines con los cuales se capturen los datos se podría trazar la carta de navegación que ancle a la seguridad de la información con custodia de los datos personales.

De esta forma la preservación de la confidencialidad permitirá establecer medidas de protección que evalúen el acceso autorizado a los datos y la gestión de los mismos, permitiendo trazar lineamientos para determinar quién puede acceder a los datos personales, mitigar el acceso a estos a través de diferentes controles e inclusive plantear como como responder en caso de que se genere alguna vulneración proveniente desde la trasgresión del acceso.

Por otro lado, atendiendo a la protección de la integridad de los datos personales, serán necesarias las medidas que permitan por un lado evaluar las consecuencias de cara a la alteración y modificación (malintencionada o no) de los datos y que, por

otro, una vez evaluados estos ítems, den pie a la generación de estrategias de seguridad que velen por la conservación de la información de manera íntegra y completa.

Finalmente, en lo que se refiere a la disponibilidad resulta uno de los pilares más importantes, tanto para la organización y su operación como ante las solicitudes particulares de los titulares de los datos personales, es por ello que desde la seguridad de la información deberá evaluarse ¿qué sucede si no son accesibles los datos personales cuando los necesitemos? Exigiendo, como tal, el establecimiento de mecanismos de protección que permitan contar con respaldos en tiempo real que garanticen el acceso a los datos, sin dilaciones y sin incumplir lo requerido por la ley.

Por consiguiente, deberá partirse de la regulación normativa, pero ello implicará la participación de diferentes áreas y la adopción de diferentes medidas que apunten al establecimiento de un sistema integral para la gestión de datos personales, cuya protección deberá estar dirigida a garantizar la protección de los titulares y sus datos, dentro de un ciclo claro del dato, en el cual debe preservarse siempre su integridad, disponibilidad y confidencialidad.

## 5. Conclusiones

1) Las organizaciones de carácter privado no están exentas de la protección de datos personales, pero el contrario la carga de estas emana desde la misma norma, por lo cual son requeridas de manera expresa para la protección de datos personales y para ello no solo tendrán que realizar la interpretación y adopción normativa a partir de una serie de principios fijados por ley, sino que tendrán establecer un sistema claro, evidente, estratégico y tangible que le permite demostrar la responsabilidad y el cumplimiento de los lineamientos determinados jurídicamente para la protección de los datos personales capturados, gestionados, almacenados y depurados.

2) La protección de datos personales al interior de las organizaciones privadas exige un proceso constante de adaptación, pues no solo debe responder a las formas tradicionales (tratamiento de información física) sino que deben sumirse riesgos y responsabilidades en una sociedad en la cual prolifera la tecnología, la cual genera por un lado agilidad en el tratamiento de datos personales, pero a su vez incrementa los riesgos y posibles vulneraciones debido a las trasgresiones dirigidas a causar lesiones o daños en la integridad, disponibilidad y confidencialidad de la información.

3) Al interior de las organizaciones privadas, la gestión de la seguridad de la información, enfocado en datos personales, debe partir de la adopción de las disposiciones normativas y cumplimiento regulatorio, que se desglose en la generación de medidas tangibles y demostrables, que se traduzcan en el involucramiento de diferentes áreas, que permitan determinar de forma clara cual es el tratamientos de los datos personales y así poder levantar estrategias de protección que tengan una visión holística que permita preservar los pilares de la información: su la integridad, disponibilidad y confidencialidad.

## Referencias


- Calderón Alateco, L. (2015) Seguridad Informática y Seguridad de la información. Universidad Piloto. Colecciones Especialización en Seguridad Informática. Págs. 1- 7. Recuperado de: http://repository.unipiloto.edu.co/handle/20.500.12277/2821
- Cárdenas-Solano, L.-J., Martínez-Ardila, H., Becerra-Ardila, L.-E. (2016). Gestión De Seguridad De La Información: Revisión Bibliográfica. El Profesional de La Información, 25(6), 931–948. https://doi-org.consultaremota.upb.edu.co/10.3145/epi.2016.nov.10
- Castillo Jiménez, C. Protección Del Derecho A La Intimidad y Uso De Las Nuevas Tecnologías De La Información. Derecho y conocimiento, vol. 1, págs. 35-48. Recuperado de: http://rabida.uhu.es/dspace/bitstream/handle/10272/1565/b1205654.pdf
- Chanamé Orbe, R. (2003). Habeas data y el derecho fundamental a la intimidad de la persona (Tesis para la Maestría, Universidad Nacional Mayor de San Marcos, Lima, Perú). Recuperada de: http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/1202/Chaname_or.pdf?sequence=1&isAllowed=y
- Colombia. Constitución política (1991), artículo 15, título II. Secretaría del Senado. 31 de diciembre de 2020
- Congreso de Colombia. (31 de diciembre de 2008). Ley Estatutaria 1266 de 2008. Diario Oficial: 47.219.
- Congreso de Colombia. (17 de octubre de 2012). Ley Estatutaria 1581 de 2012. Diario Oficial 48.587.
- Corte Constitucional. (16 de junio de 1992) Sentencia T-414. MP Ciro Angarita Baron
- Corte Constitucional. (12 de octubre de 1994) Sentencia T-443. MP Eduardo Cifuentes Muñoz

- Corte Constitucional. (05 de septiembre de 2002) Sentencia T-729. MP Eduardo Montealegre Lynett
- Corte Constitucional (17 de enero de 2011) Sentencia T- 017. MP Gabriel Eduardo Mendoza Martelo
- Corte Constitucional (13 de septiembre de 1995) Sentencia T-411. MP Alejandro Martínez Caballero.
- Corte Constitucional (20 de junio de 1995) Sentencia T 261. MP José Gregorio Hernández Galindo.
- Figueroa Suarez, J- Rodríguez Andrade, R- Bone Obando- C, Saltos Gómez, J (2017). La seguridad informática y la seguridad de la información. Polo del Conocimiento. (Edición núm. 14) Vol. 2 No 12., págs. 145-155. Recuperado de: https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf
- García González, A. (2007). La Protección De Datos Personales: Derecho Fundamental Del Siglo Xxi. Un Estudio Comparado. Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, págs.1-36. Recuperado de: http://www.scielo.org.mx/pdf/bmdc/v40n120/v40n120a3.pdf
- Gayo, M. R. (2017). Big Data: Hacia La Protección De Datos Personales Basada en Una Transparencia Y Responsabilidad Aumentadas. Revista de Derecho Comunicaciones y Nuevas Tecnologías, 17, 1–24. Recuperado de: https://doi-org.consultaremota.upb.edu.co/10.15425/redecom.17.2017.09
- Incibe- Instituto Nacional de Ciberseguridad. Protección de la información. Colección proteger tu empresa. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf
- Macías Valencia, D- Quiroz Zambrano, S. (2017). Seguridad en informática: consideraciones. Revista científica Dominio de las ciencias, Vol. 3, núm. 5, julio, págs. 676-688. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

- Monsalve Caballero, V. (2017). La Protección De Datos De Carácter Personal en Los Contratos Electrónicos Con Consumidores: Análisis De La Legislación Colombiana Y De Los Principales Referentes Europeos. Prolegómenos Derechos y Valores, 20(39), 163–195. https://doi-org.consultaremota.upb.edu.co/10.18359/prole.2729
- Muñoz Cañavate, A. (2003) Sistemas de información en las empresas. Revista Académica sobre Documentación Digital y Comunicación Interactiva. N 1, 2003. Recuperado de: file:///C:/Users/USUARIO/Downloads/Sistemas_de_informacion_en_las_empresas.pdf
- Pérez Fernández, O. (2017). El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. Recuperado de: http://hdl.handle.net/10983/14745
- Pérez Frutoso, M. J., & Gracera Cubero, J. (2018). Análisis Y Gestión Del Riesgo Operacional en Las Entidades Financieras Y Aseguradoras Una Comparativa. Revista Ibero-Latinoamericana de Seguros, 27(49), 219–245. Recuperado de: https://doi-org.consultaremota.upb.edu.co/10.11144/Javeriana.ris49.agro
- Rojas Bejarano, M. Evolución Del Derecho De Protección De Datos Personales En Colombia Respecto A Estándares Internacional. Novum Juss, vol. 8 N 1, págs. 109-137. Recuperado de: file:///C:/Users/USUARIO/Downloads/652-Texto%20del%20art%C3%ADculo-1781-1-10-20151209.pdf
- Superintendencia de Industria y Comercio. Protección de datos personales: Aspectos sobre el derecho de habeas data. Recuperado de https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf
- Velas Melo, A. (2008). El Derecho Informático Y La Gestión De La Seguridad De La Información Una Perspectiva Con Base En La Norma Iso 27 001. Revista de

Derecho, Universidad del Norte, N° 29, págs. 333-366. Recuperado de: http://rcientificas.uninorte.edu.co/index.php/derecho/article/viewFile/2700/1811