

INGRID LORENA CAMPOS VARGAS

EL DESARROLLO DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA EN LAS
POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES EN LAS UNIVERSIDADES
ACREDITADAS DE ALTA CALIDAD EN BOGOTÁ

MAESTRIA EN DERECHO INFORMATICO Y NUEVAS TECNOLOGÍAS

Bogotá, D.C., Colombia

2020

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRIA EN DERECHO INFORMATICO Y DE LAS NUEVAS TECNOLOGIAS

Rector: Dr. Juan Carlos Henao Pérez

Secretaria General: Dra. Martha Hinestrosa Rey

Director Departamento: Dra. Teresa Vargas Osorno

Director de Tesis: Adriana Castro Pinzón

Presidente de Tesis: Dra. Teresa Vargas Osorno

Jurado Sol Beatriz Calle de D'Alemán

Jurado Brenda Salas Pasuy

CONTENIDO

JUSTIFICACIÓN	5
PREGUNTA DE INVESTIGACIÓN Y OBJETIVOS	8
CAPÍTULO PRIMERO: El Principio De Responsabilidad Demostrada En Las Políticas De Protección De Datos Personales	10
1. Guía para la implementación del Principio de Responsabilidad Demostrada	11
Conclusión	18
CAPÍTULO SEGUNDO: Cumplimiento Del Principio De Responsabilidad Demostrada En Las Políticas De Protección De Datos Personales En Las Universidades Acreditadas De Alta Calidad En Bogotá Colombia	20
1. Los sujetos que se enmarcan en el tratamiento de datos personales en Colombia	22
2. Política de protección de datos	29
3. Instituciones de Educación Superior (IES).	31
4. Instituciones de alta calidad en Bogotá	33
Conclusión	41
CAPÍTULO TERCERO: Propuesta Contenido Mínimo Para El Diseño De Un Manual Interno De Normas Y Lineamientos Para Cumplir Con El Principio De Responsabilidad Demostrada	42

1. Europa	43
1.1 España	46
1.2 Alemania	48
2. América	48
2.1 Estados Unidos	48
3. Colombia	50
4. Elementos o criterios para la construcción de la propuesta	51
Conclusión	72
Conclusiones finales	73
REFERENCIAS BIBLIOGRÁFICAS	74

Lista de Tablas y Figuras

Tabla 1	8
Tabla 2	11
Tabla 3	18
Figura 1	20
Figura 2	22
Figura 3	29
Figura 4	33
Figura 5	33
Figura 6	36
Tabla 4	40
Figura 7	41
Figura 8	42
Figura 9	48
Figura 10	51
Figura 11	56

JUSTIFICACIÓN

Para conocer cómo se desarrolla del principio de responsabilidad demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia, es necesario relacionar aspectos importantes sobre la comprensión, la asimilación y el conocimiento sobre dicho principio.

Las Instituciones de Educación Superior (IES), recolectan, administran, almacenan y en general realizan tratamiento de una gran cantidad de información de los aspirantes, los estudiantes, sus egresados, proveedores, empleados, contratistas, y en general a toda la comunidad universitaria que hace parte de las IES estudiadas, entonces es en las IES donde se delimita la población que tiene incidencia directa en la aplicación del principio de responsabilidad demostrada.

Para el logro de la presente investigación, se parte del análisis del desarrollo y la aplicación del principio de responsabilidad demostrada en las Universidades Acreditadas de alta calidad de Bogotá , para lo cual, se muestra cómo dichas IES implementan este principio, o si se requiere proponer acciones para lograr el cumplimiento del mismo, y así garantizar la observancia de las normas nacionales e internacionales vigentes y con los estándares éticos necesarios para permitir un pleno cumplimiento del derecho de protección de datos personales.

Estas universidades delimitadas como objeto de estudio en un primer momento por estar acreditadas de alta calidad, lo que garantiza su aseguramiento a la calidad en la educación superior, políticas claras frente a la docencia, investigación y extensión, además de delimitar el territorio a la Ciudad de Bogotá por ser un referente a nivel nacional en acceso y calidad de la educación.

Para su logro, el Consejo Nacional de Acreditación (CNA) (s.f) y el Ministerio de Educación de Colombia, establecen una serie de condiciones para que las universidades sean acreditadas de alta calidad; estas condiciones están directamente relacionadas con docentes, egresados y estudiantes, investigación, autoevaluación, currículo, entre otras, en estas condiciones deben brindar un correcto y adecuado uso de un programa responsable de protección de datos personales. Es aquí, donde la investigación toma relevancia, porque analiza el principio de responsabilidad demostrada en el tratamiento de datos personales en la IES acreditadas de alta calidad en la ciudad de Bogotá.

El derecho de protección de datos personales como un derecho fundamental que reviste de importancia en la sociedad de la información propende por el respeto a la Dignidad Humana y está relacionado con el uso, administración, almacenamiento de la información propia de las personas.

Los datos personales que se recolectan para el desarrollo de las actividades misionales (docencia, investigación y servicio) de las Universidades, son recolectados bajo el cumplimiento de las normas de protección de datos personales con un enfoque de responsabilidad demostrada que propenda por la autorregulación, la prevalencia de principios éticos y la generación de una cultura de respeto por los datos personales no solo en los docentes e investigadores, sino también en toda la comunidad universitaria, que finalmente replican esta cultura.

No obstante, la forma como en Colombia se ha asumido la protección de datos personales y la aplicación de la Ley 1581 de 2012 en el sector de la educación superior, tiene su enfoque para que las personas conozcan, actualicen y rectifiquen las informaciones que se hayan recogido sobre ellas¹, así, es importante crear una cultura de respeto por los datos personales que efectivamente tenga como centro los derechos del ser humano.

Para esto, se toma la legislación a nivel nacional e internacional, porque son estos el soporte teórico de donde se desprende la comprensión a nivel nacional, es importante visualizar que estos referentes, son la hoja de ruta que han nutrido la discusión a nivel nacional, además de lo anterior, contar con referentes claros, evidencia la forma y el modo de cómo se debe implementar el principio de Responsabilidad Demostrada en Colombia y más concretamente en la IES objeto de estudio; estos antecedentes, realizan aportes relevantes para lograr articular conceptos claves, entorno a la comprensión de la protección de datos personales y el principio de responsabilidad demostrada.

El trabajo adquiere especial relevancia al establecer el cumplimiento del principio de Responsabilidad Demostrada en las IES, dado que, son un elemento de análisis fundamental para comprender la aplicación de este, también la reflexión se da, entorno a la propuesta de un manual que sea una hoja de ruta tanto para la comprensión como para el entendimiento de dicho principio.

¹ Artículo 1. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

PREGUNTA DE INVESTIGACIÓN

¿Cómo se desarrolla el Principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia?

¿Cómo se evidencia el Principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia?

OBJETIVOS

Objetivo general: Indagar sobre el desarrollo del principio de responsabilidad demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia.

Evidenciar el Principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia.

Objetivos específicos:

1. Identificar el principio de Responsabilidad Demostrada en las políticas de protección de datos personales.

Pregunta: En qué consiste el principio de Responsabilidad Demostrada en las políticas de protección de datos personales.

Título Capítulo Primero: El principio de Responsabilidad Demostrada en las políticas de protección de datos personales.

2. Establecer el cumplimiento del principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia.

Pregunta: ¿Cómo se cumple el principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia?

Título Capítulo Segundo: Cumplimiento del principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia.

3. Establecer el contenido mínimo para el diseño de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada para su comprensión y aplicación, acorde con las actividades misionales de las universidades acreditadas de alta calidad en Bogotá Colombia.

Pregunta: ¿Cuál es el contenido mínimo de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada en las universidades acreditadas de alta calidad en Bogotá Colombia?

Título Capítulo Tercero: Propuesta contenido mínimo para el diseño de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada.

Capítulo Primero: El principio de Responsabilidad Demostrada en las políticas de protección de datos personales.

El presente capítulo, busca identificar el principio de Responsabilidad Demostrada en las políticas de protección de datos personales a través de su conceptualización, también, muestra las organizaciones han elaborado documentos relevantes frente a la protección de datos y se enuncia la Guía para la implementación del Principio de Responsabilidad Demostrada, para ello plantea la pregunta y el objetivo que se muestran a continuación:

Tabla 1

Encuadre del capítulo

Pregunta	En qué consiste el principio de Responsabilidad Demostrada en las políticas de protección de datos personales.
Objetivo	Identificar el principio de Responsabilidad Demostrada en las políticas de protección de datos personales.

Fuente: Construcción propia

Para identificar el principio de Responsabilidad Demostrada en las políticas de protección de datos personales, es necesario en un primer momento, definir dicho principio:

El término accountability (responsabilidad) proviene del mundo anglosajón y a pesar de las diferentes acepciones que puedan darse de él, se ha entendido que en el área de la protección de datos dicha expresión se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente. (Remolina y Álvarez, 2018, p.p. 28-29).

Este principio, refiere al modo y forma de cómo se lleva a la práctica la protección de datos en las organizaciones, además establece el reto permanente de cualquier organización para su cumplimiento, al respecto:

Garantizar la aplicación efectiva y práctica de lo que ordenan las normas sobre protección de datos es un reto permanente de cualquier organización. El principio de responsabilidad cobra cardinal importancia para lograr ese propósito. Dicho principio exige que los responsables y encargados del tratamiento de datos, implementen medidas apropiadas, efectivas y verificables que les permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, el Programa Integral de Gestión de Datos Personales (PIGDP) se constituye en un mecanismo operativo para realizar todo lo necesario con miras a garantizar el debido tratamiento de los datos personales. (Remolina y Álvarez, 2018, p. 29).

1. Guía para la implementación del Principio de Responsabilidad Demostrada

En septiembre de 2013 las guías de la OCDE recogen un principio fundamental conocido como responsabilidad demostrada (accountability en inglés), según el cual una entidad que recoge el tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos.

La versión de 2013, establece un nuevo aporte sobre implementación del principio de responsabilidad demostrada respecto a las anteriores. En este sentido, los responsables del tratamiento deben contar con un programa de gestión de datos personales y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en la organización (Guía para la protección de la privacidad y los flujos transfronterizos de datos personales, 1980). Este

concepto que es implementado para el uso y el tratamiento de los datos personales implica que, se resalte la importancia de y el papel que juega el responsable del tratamiento de los datos.

Es el llamado a implementar medidas dentro de la organización que le permitieran cumplir con el resto de los principios consagrados, trabajando en esa línea y reconociendo la importancia de un enfoque basado en el compromiso de la organización con incrementar sus estándares de protección para garantizar a los ciudadanos un tratamiento idóneo de su información personal.

El entendimiento del principio de responsabilidad demostrada, está ligado a su incorporación en las organizaciones y su aplicación en las mismas por esto se trae al texto, los principales documentos, que se han elaborado frente a la protección de datos, a nivel internacional; esto, con el fin de sustentar la importancia de estudios referentes al tema que puedan nutrir el análisis:

Tabla 2

Documentos sobre protección de datos

Organización	Principales documentos
Red Iberoamericana de Protección de Datos (RIPD)	Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017)
Unión Europea (UE)	1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); 2. Protocolos adicionales al Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001 y 2018); 3. Carta de los Derechos Fundamentales de la Unión Europea (2000); 4. Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981)
Organización de Estados Americanos (OEA)	Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015)
Organización para la Cooperación y el Desarrollo Económicos (OCDE)	Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980)
Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP)	Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal –Resolución de Madrid– (2009)
Foro de Cooperación Económica Asia Pacífico (APEC)	Marco de privacidad APEC (2004) APEC Cross Border Privacy Rules (CBPR) APEC Cross Border Privacy Enforcement Arrangement (CPEA)
Organización de las Naciones Unidas (ONU)	Resolución 45/95 del 14 de diciembre de 1990. Principios rectores para la reglamentación de los ficheros computarizados de datos personales

Fuente: Remolina, 2015.

Así, se tiene que el derecho de protección de datos personales en el marco de regulación europea, es un derecho fundamental y autónomo que ha tenido una evolución normativa para adaptarse a los nuevos desafíos de la sociedad de la información que tiene como reto lograr la estandarización del entendimiento de su alcance a nivel mundial.

Esta tendencia ha sido influyente en los países de América Latina y en especial en Colombia, se ha tomado como referente el modelo europeo.

Dicho modelo, consiste en el que se considera el procesamiento automático de los datos personales de los individuos en la Convención N° 108 del Council Europeo el 28 de enero de 1981 (Martínez-Martínez, 2018) y también lo que propone en el Artículo 8 de la Convención Europea de los Derechos Humanos. (ECHR, por sus siglas en inglés) (Consulado de Europa, 2010). De este modo:

El principio de responsabilidad demostrada también se ha incluido en las regulaciones de algunos países latinoamericanos, como México y Colombia. En este último, por ejemplo, además de lo establecido en el Decreto 1377 del 2013, el Decreto 1413 del 2017 se refiere expresamente a la responsabilidad y los programas integrales de gestión de datos en los siguientes términos: Primero, obliga a los “operadores de servicios ciudadanos digitales” a adoptar “medidas apropiadas, efectivas y verificables que le[s] permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales”. Luego, ordena a dichos operadores “crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales”. Finalmente, establece que el PIGD deberá cumplir con “las instrucciones de la Superintendencia de Industria y Comercio, en particular, la guía para la implementación del principio de responsabilidad demostrada (accountability) de dicha entidad”. (Remolina y Álvarez, 2018, p. 32).

La importancia de la cita anterior radica en que muestra cómo se han incluido regulaciones en cuanto a la toma de medidas efectivas y verificables sobre la norma de tratamiento de datos personales.

También, la Ley 1581 de 2012, es anterior al GDPR, consagra elementos previstos en esta nueva norma, como la responsabilidad demostrada o proactiva, por cuanto el legislador colombiano tuvo en cuenta los desarrollos jurisprudenciales de la anterior directiva europea.

A continuación, se enuncia el Artículo 1 de la Ley 1581, cuya relevancia, radica en evidenciar el derecho constitucional frente al uso de la información en bases de datos:

ARTÍCULO 1o. OBJETO. La presente ley 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. (Congreso de la República, 2012).

En Colombia la carga del principio de responsabilidad demostrada se presenta en el capítulo VI del decreto 1377 de 2013, por el cual se reglamenta la Ley 1581 de 2012 en él se desarrollan los lineamientos de los programas de responsabilidad demostrada, de manera expresa. Los responsables del tratamiento de datos en Colombia, deben además de tener políticas de protección de datos personales, contar con los procesos, procedimientos y controles necesarios para demostrar a la autoridad de control que las políticas son efectivas para garantizar el derecho a la protección de datos personales:

Artículo 26. del Decreto 1377 de 2013 acerca de la Responsabilidad Demostrada frente al tratamiento de datos personales:

Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han

implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente: 1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente. 2. La naturaleza de los datos personales objeto del tratamiento. 3. El tipo de Tratamiento. 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

En este sentido, las instituciones de educación superior deben de acuerdo al artículo anterior proveer evidencias acerca de los procedimientos y estrategias por medio de los cuáles brindan tratamiento a los datos personales que reúnen.

Para Colombia la jurisprudencia establece las características de los datos personales:

La jurisprudencia constitucional ha precisado que las características de los datos personales son las siguientes: i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación. (Corte Constitucional, 2011).

La protección de datos personales contemplada en el principio de responsabilidad demostrada, es uno de los elementos clave para garantizar la seguridad y el acceso seguro a la sociedad de la información, para su comprensión y con el fin de dar antecedentes pertinentes se

muestran varias miradas sobre el concepto, para luego realizar un encadenamiento conceptual consecuente:

La protección de datos personales y la privacidad son términos que se interrelacionan al hablar de la Regulación General para la Protección de Datos o GDPR-por sus siglas en inglés-, no obstante, existen diferencias sustantivas en ambos. Apelar a la “privacidad” de un individuo generalmente se refiere a la protección del *espacio personal* del mismo, mientras que la protección de los datos personales hace énfasis a las limitaciones o condiciones en el procesamiento de los datos relacionados a la identificación de un individuo. (Gligora, Debeljak & Kadoić, 2019).

También, la protección de datos muestra la relación entre las instituciones y el ciudadano debe estar mediada, por el uso responsable y consecuente, los datos están relacionadas con la identidad de la persona, en todos los casos, la información allí consignada, está directamente ligada a la realidad de los ciudadanos:

Referir a los datos personales incluye hablar de nombre, dirección, correo electrónico, número telefónico, etiquetas, fotos, videos, información biométrica, genética, datos con respecto a la educación, al salario, historial crediticio, información de cuentas de banco y muchos otros factores relacionados con los individuos y por medio de los que se puede conocer o determinar su identidad.

Su origen normativo, reside en la Declaración Universal de los Derechos Humanos (2015), en su artículo 8, de ahí, nace gran parte de la normativa y se tiene como principio general y básico para el tratamiento de datos, sobre esto, Grava afirma:

El derecho a la protección de datos tiene su origen en el derecho a la privacidad, reconocido en el Artículo 12 de la Declaración Universal de los Derechos Humanos (1948) y en el Artículo 8 del Convenio Europeo de Derechos Humanos (1950) del Consejo de Europa, aunque existen hoy muchos autores que consideran privacidad y protección de datos como conceptos distintos (Grava, 2017; citado en Varela y Ameneiros, 2018, p. 688).

Para esto la Ley Colombiana de protección de datos (2012), como su nombre lo indica, protege el derecho que tienen las personas a brindar acceso a sus datos personales, y del mismo modo, a actualizar y rectificar la información que allí se consigna y que posteriormente es guardado en las bases de datos que se utilizan, conocido como el derecho de Habeas Data.

A continuación, se muestra la definición de datos personales que da cuenta de la información asociada a una persona:

Cuando se habla de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos. (Hernández y Zavala, 2018, p. 223)

Conclusión

A razón de lo anterior, se puede resaltar el punto de partida del Principio de Responsabilidad Demostrada en la recolección de información y datos personales que realizan distintas entidades y organizaciones como las Instituciones de Educación Superior, siendo así, éste principio se pregunta por aquellas prácticas que evidencian el modo como se dispone dicha

información y las estrategias o modos de garantizar su protección. Considerar pues el Principio de Responsabilidad Demostrada, equivale como se detalló, a comprender la manera en que se conceptualiza éste según los documentos institucionales que regulan su práctica, y así mismo, relacionarla a la incorporación mediante programas de gestión de datos personales que permitan garantizar el Principio de Responsabilidad Demostrada en las políticas de protección de datos personales más allá de modelos europeos replicados, sino en cambio, como medidas apropiadas y efectivas al interior del ámbito colombiano.

Capítulo Segundo: Cumplimiento del principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia.

El siguiente capítulo, identifica el cumplimiento de la responsabilidad demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia. Para ello, enuncia el Derecho de Habeas Data y reconocer los sujetos que enmarcan en el tratamiento de datos personales en Colombia, la definición la descripción de responsables y encargados:

Tabla 3

Encuadre del capítulo

Pregunta	¿Cómo cumplen el principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia?
Objetivo	Identificar el cumplimiento del principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia.

Fuente: Construcción propia

Para identificar el cumplimiento del principio de Responsabilidad Demostrada en las políticas de protección de datos personales en las universidades acreditadas de alta calidad en Bogotá Colombia, en primera medida y considerando la Ley 1581 de 2012, se especifica el Derecho de Habeas Data que consiste en: Requisito de consentimiento libre, previo, expreso e

informado del titular del dato de excepción a la autorización o consentimiento previo para el uso del dato no vulneran la constitución.

El consentimiento del titular de la información es un presupuesto para la legitimidad constitucional de los procesos de administración de datos personales, tratándose de un consentimiento calificado: ya que debe ser previo, esto es, que la autorización debe ser suministrada en una etapa anterior a la incorporación del dato; expreso, en la medida que debe ser inequívoco; e informado, toda vez que el titular no sólo debe aceptar el tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. (...) los casos en que no es necesaria la autorización, específicamente cuando: la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, los datos de naturaleza pública, los casos de urgencia médica o sanitaria, tratamiento autorizado por la Ley para fines históricos, estadísticos o científicos y datos relacionados con el registro civil de las personas, casos éstos en los que existen importantes intereses constitucionales que justifican tal limitación. (República de Colombia, 2011).

Así mismo, se hace importante identificar claramente los sujetos que hacen parte en el tratamiento de datos personales en Colombia, con el fin de establecer la articulación con el principio de responsabilidad demostrada, en las universidades acreditadas de alta calidad en Bogotá Colombia; es decir, se parte de la generalidad para entender el sistema, y lograr entender la carga de dicho principio:

1. Los sujetos que se enmarcan en el tratamiento de datos personales en Colombia:



Figura 1. Sujetos que enmarcan el tratamiento de datos personales en Colombia. Fuente: Construcción propia

A continuación, se describen cada uno de los sujetos que tienen que ver en el proceso de tratamiento de datos y que, participan en el:

El titular: Persona Natural que es titular de los datos personales y cuyos datos son objeto de tratamiento.

El responsable: Persona Natural o Jurídica, pública o privada, que por sí misma o en asocio con otro decida sobre la base de datos o realice tratamiento de datos.

El encargado: Persona Natural o Jurídica, pública o privada, que por sí misma o en asocio con otro decida sobre la base de datos o realice tratamiento de datos personales por cuenta del responsable del tratamiento (Congreso de Colombia, 2012).

De manera concreta las Universidades pueden ser responsables o encargadas del tratamiento de datos que recolecta o almacenan de sus grupos de interés.

Para comprender el contenido y el alcance del derecho de protección de datos personales es importante tener claros algunos conceptos propios de la ley, y que son los que determinan la forma de cómo proceder. Se traen al texto definiciones importantes de la Ley 1581 (Congreso de Colombia, 2012):

Tabla 4

Definiciones en el marco del derecho de protección de datos personales

Definición	Descripción
Autorización	Consentimiento previo, expreso y debidamente informado del titular para llevar a cabo el tratamiento de datos personales.
Base de Datos	Conjunto organizado de datos personales que sea objeto de tratamiento.
Dato personal	Cualquier información vinculada o que pueda asociarse a una persona o varias personas naturales determinadas o determinables.
Dato sensible	De acuerdo con el artículo 5 de la ley 1581 de 2012, se entiende por éstos aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como aquellos que revelan origen racial o étnico, la orientación política
Menores de Edad	Persona natural menor de 18 años. Los datos de los menores tienen una especial protección y en cuanto a medidas de seguridad para su protección deben tener las más altas medidas.
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso circulación o supresión.

Fuente: Construcción propia

En la siguiente figura, se muestran los principios jurídicos de la Ley 1581 de 2012, en ella el conector (is associated with), significa “en asociación con”, y hace referencia a la relación que existe entre ellos para la ejecución de dicha ley:

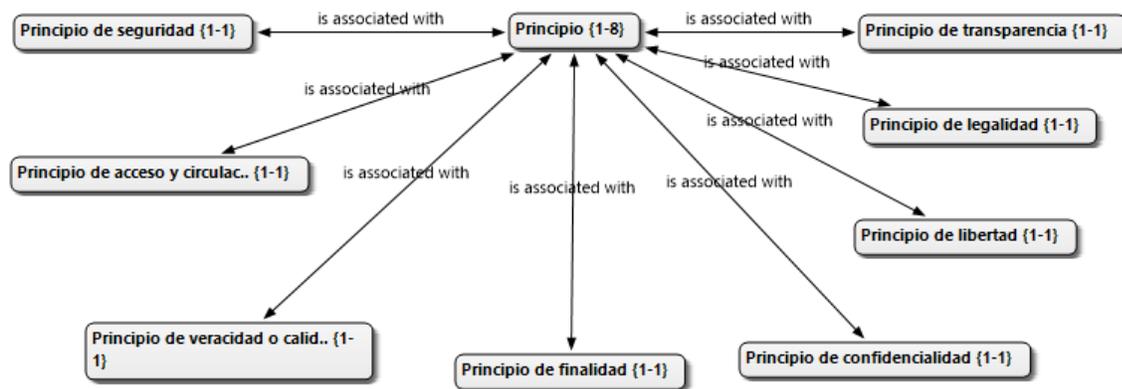


Figura 2. Principios jurídicos de la Ley 1581 de 2012. Fuente: Construcción propia.

- Principio de legalidad: se refiere principalmente a que el tratamiento de datos personales es una actividad reglada y por tanto de interpretación restrictiva.
- Principio de finalidad: se refiere a que el tratamiento de datos debe realizarse para el desarrollo de una actividad legítima la cual deber ser informada al titular, de manera previa y expresa.
- Principio de libertad: el cual consiste en la potestad autónoma y única de cada titular de autorizar o no el tratamiento de sus datos personales.
- Principio de veracidad o calidad: Se refiere a que la información personal sujeta a tratamiento debe ser veraz, exacta, actualizada, comprobable y actualizada.
- Principio de transparencia: Consiste en que el responsable o el encargado tienen el deber de siempre informar al titular que están haciendo con sus datos.
- Principio de acceso y circulación restringida: El uso o tratamiento de los datos debe limitarse a lo que señala la finalidad y que el acceso a los mismos debe ser controlado.

- Principio de seguridad: Los datos personales deben estar almacenados con medias de seguridad técnicas, humanas y administrativas que atenúen los riesgos de fuga de información o adulteración de esta que genere un daño o perjuicio al titular de los datos o que lo ponga en riesgo.
- Principio de confidencialidad: Toda persona que intervenga en el tratamiento de datos está obligada a guardar absoluta reserva respecto a los datos personales que conozca en ejercicio de sus funciones, obligación que persiste incluso una vez terminada la relación contractual con el responsable.

Tal como se puede evidenciar el principio de responsabilidad demostrada no se encuentra expresamente consagrado en la citada ley, sin embargo, es considerado un desarrollo del principio de transparencia.

Así mismo, los derechos que establece la ley y que puede ejercer cualquier titular de acuerdo con el artículo 10 de la Ley 1581 de 2012 (Congreso de Colombia, 2012) son:

- Conocer, actualizar y rectificar sus datos personales frente a los responsables o encargados. Solicitar prueba de la autorización, salvo cuando expresamente se exceptúe como requisito para el Tratamiento.
- Este derecho se ejerce mediante el mecanismo de consulta que consiste en la facultad que tiene cualquier titular de consultarle al responsable o a sus encargados que tipos de datos personales tiene y solicitar la corrección de estos.

En relación con las excepciones a la solicitud de autorización, estas, se encuentran reguladas de manera expresa en el artículo 10 de la ley 1581, indicando que no se requiere autorización cuando la información es solicitada por una autoridad pública en ejercicio de sus funciones, en

este caso, el responsable de los datos debe asegurarse que la finalidad para la cual se solicita la información se encuentre en las funciones expresas de la entidad, e igualmente debe informarle sobre el garantizar el cumplimiento de todos los principios de la ley de habeas data.

Una excepción a la solicitud de autorización se trata de una solicitud de datos de naturaleza pública, excepción que ofrece dificultades en su aplicación, por cuanto la definición de datos de naturaleza pública adopta por el legislador colombiano es poco precisa dado que, establece que los datos de naturaleza pública son aquellos que no son considerados privados ni semiprivados.

Otra excepción son los datos relacionados con el registro civil, que en la práctica han sido tomados como datos de naturaleza pública.

También, cuando se presenta urgencia médica o sanitaria por cuanto prevalecen otros derechos y el tratamiento de datos con fines históricos, estadísticos o científicos, en este último caso siempre que se apliquen medidas de anonimización adecuadas (Congreso de Colombia, 2012):

- Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley. Este derecho para su ejercicio tiene como requisito de procedibilidad que el titular haya realizado la respectiva consulta o queja ante el responsable o encargado del tratamiento.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. Este derecho debe analizarse de manera armónica en cuanto a que la solicitud de supresión sería procedente

siempre que el dato no se requiera para garantizar otro derecho o para que sobre todo las entidades que cumplen función pública.

En correlación con los derechos y en la medida en que una vez el titular autoriza el tratamiento de sus datos, al responsable por el uso de la información le surgen unas obligaciones para garantizar al Titular el pleno y efectivo ejercicio del derecho de hábeas data (Congreso de Colombia, 2012).

- Solicitar y conservar copia de la respectiva otorgada por el Titular. Esta obligación en la práctica genera al interior de las organizaciones grandes desafíos frente a la administración de los consentimientos, pues no es solo obtener la autorización del titular, sino que el responsable debe conservar prueba de la misma para ante cualquier reclamación tener claro que le fue autorizado, así mismo, es importante su conservación pues frente a una visita de inspección y vigilancia de la Superintendencia de industria y comercio en adelante (SIC), es solicitada para acreditar que el uso de la información está siendo el autorizado por el titular.
- Informar debidamente al Titular sobre la finalidad de las **autorizaciones**, la recolección y los derechos que le asisten por virtud de la autorización otorgada.

Esta obligación define o determina los tres elementos mínimos que debe incluir cualquier texto de autorización de tratamiento de datos, siempre que no contenga datos sensibles, pues en este último caso la norma señala que se deberá agregar la advertencia de que es facultativo la autorización de datos sensibles que no sean necesarios para la prestación del servicio.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Como se menciona anteriormente, el principio de seguridad debe versar sobre los medios tecnológicos y los procesos administrativos.

Las medidas de seguridad tecnológicas pues es importante señalar que en la norma en cuanto a las medidas de seguridad tecnológicas no señala ningún referente para garantizar esta obligación, para esto las buenas prácticas han referido a la norma ISO 27001.

En Colombia, la Superintendencia de Industria y Comercio no ha reconocido manera expresa dicha norma como referente e incluso algunos sectores consideran que la SIC, se encuentra en mora de regular o adoptar un referente para cumplir con esta práctica en una sociedad hiper-conectada.

En cuanto a los controles de seguridad administrativos y de los empleados la buena práctica señala que las organizaciones deben contar con procedimientos documentados de notificación de incidentes de seguridad y con acuerdos de confidencialidad con sus empleados y contratos de transmisión o transferencia de datos que garanticen la seguridad de los datos personales (Congreso de Colombia, 2012).

- Garantizar que la **información que se suministre al Encargado** del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

Por tal motivo, se debe contar con un procedimiento que garantice que la información de los titulares está actualizada y verificar que la información que se entrega al encargado es la correcta.

- Actualizar la información e informar al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la ley.

Al respecto la norma establece unos plazos claros para dar respuesta a las solicitudes de los titulares, los cuales se deben cumplir so pena de que el titular inicie su proceso de reclamación ante la SIC.

2. Políticas de protección de datos.

El capítulo III del Decreto Reglamentario 1377 de 2013, compilado en el Decreto 1074 de 2015, versa sobre la importancia, el contenido y el alcance de las políticas de protección de datos:

Artículo 13. Políticas de Tratamiento de la información. Responsables del tratamiento deberán desarrollar políticas de tratamiento de datos personales y verificar porque esto se cumpla, deben ser de acceso público de manera digital y físico, con un lenguaje claro. Debe incluir mínimamente lo siguiente: 1. Datos básicos de contacto, 2. Información sobre el tratamiento de

los datos y finalidad, 3. Derechos como titular, 4. Persona o área encargada de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización, 5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización. 6. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos. (Ministerio de Comercio, Industria y Turismo, 2015)

Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el artículo 5° del presente decreto, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas.

Así mismo, la recolección de datos personales es hoy fundamental para las relaciones contractuales, el procedimiento para obtener los y la relación con los bienes y servicios de las organizaciones de tipo económico, social o una solicitud de información, todo lo anterior, debe realizarse garantizando el cumplimiento de medidas de seguridad y controles efectivos que impidan la fuga de información personal e incluso la afectación de otros derechos también considerados como fundamentales.

Los datos personales conforman la información necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios. Así, por ejemplo, cuando se hace una solicitud de crédito ante una entidad financiera, se requiere diligenciar formularios con nuestra información personal, o cuando se hace una compra y para realizar la factura de venta solicitan datos como el número de documento de identidad, correo

electrónico, dirección y teléfono de contacto, entre otros”. (Hernández y Zavala, 2018, p. 223).

También se establecen los tipos de datos y las bases de datos a las que no les aplican la Ley:

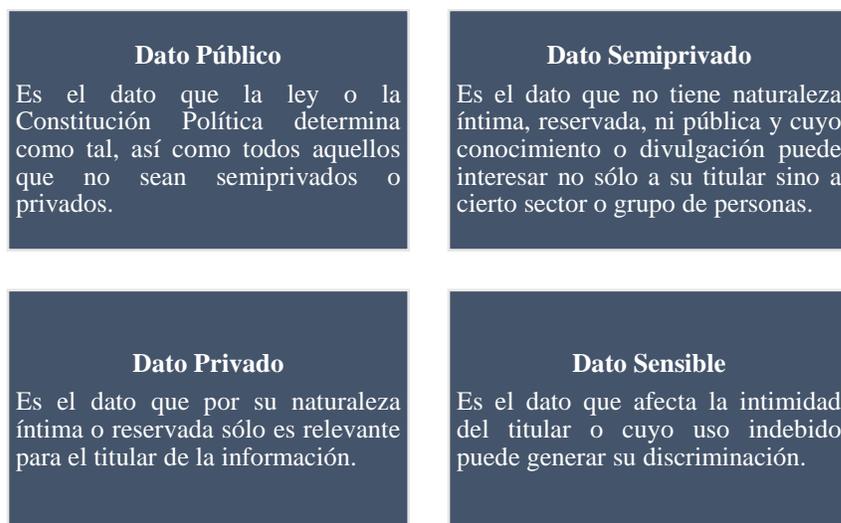


Figura 3. Tipos de datos. Fuente: Superintendencia de Industria y Comercio, 2015. Construcción propia.

Es así que el derecho a la protección de datos personales se puede entender como el poder que tiene la persona de disponer de ellos y controlarlos, decidiendo cuáles proporcionará a un tercero, ya sea un particular o el Estado, para así saber quién los posee, contando en todo momento con la facultad de acceder a ellos, rectificarlos, cancelarlos u oponerse a su posesión o uso. (Hernández y Zavala, 2018, p. 223)

3. Instituciones de Educación Superior (IES)

Considerando el contexto colombiano y haciendo relación directa con las Instituciones de Educación Superior (IES), la Ley 30 de 1992 en el Capítulo IV, regula las tipologías de Instituciones de Educación Superior, según su carácter académico, clasificándolas en Instituciones técnicas, Instituciones Tecnológicas, Instituciones Universitarias y Universidades;

en especial el Artículo 21² establece que solo las Universidades y las Instituciones Universitarias y escuelas tecnológicas, son las autorizadas para ofrecer programas de Maestría, doctorado y posdoctorado.

Universidades, son aquellas que acreditan un desempeño con criterio de universalidad en las siguientes actividades: La investigación científica o tecnológica; la formación académica en profesiones o disciplinas y la producción, desarrollo y transmisión del conocimiento y de la cultura universal y nacional.

De acuerdo con el tipo de persona jurídica el artículo 98 de la citada ley³, consagra: Las instituciones privadas de Educación Superior deben ser personas jurídicas de utilidad común, sin ánimo de lucro, organizadas como corporaciones, fundaciones o instituciones de economía solidaria.

El artículo 633, del código civil colombiano, define las personas jurídicas como una ficción jurídica de creación legal capaz de ejercer derechos y contraer obligaciones civiles y de ser representada judicialmente y extrajudicialmente las cuales se rigen de acuerdo a la ley y a sus propios estatutos.

² Ley 30 de 1992 Artículo 21. Solamente podrán ser autorizadas por el Ministro de Educación Nacional para ofrecer programas de maestría, doctorado y post-doctorado y otorgar los respectivos títulos, previo concepto favorable de] Consejo Nacional de Educación Superior (CESU), aquellas universidades que satisfagan los requisitos contemplados en los artículos 19 y 20. Parágrafo. Podrán también ser autorizadas por el Ministro de Educación Nacional para ofrecer programas de maestrías y doctorados y expedir los títulos correspondientes, las universidades, las instituciones universitarias o escuelas tecnológicas, que sin cumplir con el requisito establecido en el literal b) del artículo 20, cumplan con los requisitos de calidad según el Sistema Nacional de Acreditación, en los campos de acción afines al programa propuesto, previo concepto favorable del Consejo Nacional de Educación Superior (CESU).

³ Ley 30 de 1992 en el Capítulo IV. Artículo 98

Las personas jurídicas sin ánimo de lucro son aquellas personas jurídicas que nacen por voluntad de sus asociados o por la libertad de disposición de bienes de los particulares para la realización de fines altruista, gremiales o de beneficio comunitario.

Los tipos más comunes de entidades sin ánimo de lucro son las fundaciones y las corporaciones o asociaciones, las primeras son creadas por la voluntad de una persona o varias personas acerca de su constitución, organización, fines y medios para alcanzarlos con un fin específico, el cual es altruista y cuya voluntad es irrevocable una vez se ha obtenido el reconocimiento como persona jurídica requiere necesariamente la afectación de un patrimonio por sus fundadores.

Las corporaciones o asociaciones son entes jurídicos que surgen del acuerdo de la pluralidad de voluntades vinculadas mediante aportes en dinero especie o actividad, en con el fin de realizar un beneficio social extraeconómico que puede contraerse a los asociados a un gremio o un grupo social en particular. Su régimen es estatutario y sus decisiones se derivan de la voluntad de sus miembros.

De acuerdo con el origen de los recursos económicos, la constitución de las Universidades se clasifica así, de conformidad con el artículo 23 de la Ley 30 de 1992: “Por razón de su origen, las instituciones de Educación Superior se clasifican en: Estatales u Oficiales, Privadas y de Economía Solidaria.” (Congreso de la República de Colombia, 1992).

4. Instituciones de alta calidad en Bogotá

La importancia de esta investigación, sobre las políticas de protección de datos personales en las Universidades acreditadas en alta calidad en Bogotá radica en mostrar el desarrollo y apropiación efectiva del este derecho, garantizando un cumplimiento adecuado de acuerdo con el principio de responsabilidad demostrada.

También, es importante mencionar que de acuerdo con el Consejo Nacional de Acreditación CNA una institución acreditada de alta calidad es aquella que:

La acreditación es el reconocimiento por parte del Estado de la calidad de instituciones de educación superior y de programas académicos, es una ocasión para valorar la formación que se imparte con la que se reconoce como deseable en relación a su naturaleza y carácter, y la propia de su área de conocimiento. También es un instrumento para promover y reconocer la dinámica del mejoramiento de la calidad y para precisar metas de desarrollo institucional y de programas. El proceso de Acreditación se desarrolla a través de la evaluación de la calidad realizada por la institución misma (autoevaluación), por pares académicos externos que pueden profundizar en la naturaleza de lo que se evalúa (heteroevaluación) y por el Consejo Nacional de Acreditación (evaluación final); el proceso culmina con el reconocimiento público de la calidad por parte del Ministerio de Educación Nacional. (Consejo Nacional de Acreditación, s.f.)

De acuerdo con el Sistema Nacional de información de la Educación Superior, en adelante SNIES; se cuenta con un reporte de Universidades acreditadas de alta calidad, para la ciudad de Bogotá y que son la hoja de ruta para analizar cada uno de los recursos que tienen entorno al tratamiento de datos personales:

Nombre Institución	Estado	Principal/Secundional	Sector	Carácter Académico	Departamento Domicilio
COLEGIO MAYOR DE NUESTRA SEÑORA DEL ROSARIO	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
FUNDACION UNIVERSIDAD DE BOGOTA - JORGE TADEO LOZANO	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
PONTIFICIA UNIVERSIDAD JAVERIANA	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD ANTONIO NARIÑO	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD CATOLICA DE COLOMBIA	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD CENTRAL	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD DE LOS ANDES	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD DE SAN BUENAVENTURA	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD DISTRITAL-FRANCISCO JOSE DE CALDAS	ACTIVA	PRINCIPAL	OFICIAL	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD EAN	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD EL BOSQUE	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD EXTERNADO DE COLOMBIA	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD LIBRE	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD MILITAR- NUEVA GRANADA	ACTIVA	PRINCIPAL	OFICIAL	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD NACIONAL DE COLOMBIA	ACTIVA	PRINCIPAL	OFICIAL	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD PEDAGOGICA NACIONAL	ACTIVA	PRINCIPAL	OFICIAL	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD SANTO TOMAS	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C
UNIVERSIDAD SERGIO ARBOLEDA	ACTIVA	PRINCIPAL	PRIVADA	UNIVERSIDAD	BOGOTA D.C

Figura 4. Universidades acreditadas de alta calidad. Fuente: Sistema Nacional de Información de la Educación Superior (SNIES), 2019.

Así mismo, se muestra una figura de seguimiento, en donde se establece cada uno de los elementos que incluyen las políticas de las IES consultadas, en la que se inicia con las definiciones y seguidamente muestra, los elementos que enmarcan un procedimiento claro en donde cada uno de ellas toma especial importancia toda vez que cada una de las definiciones aporta al tratamiento de datos:

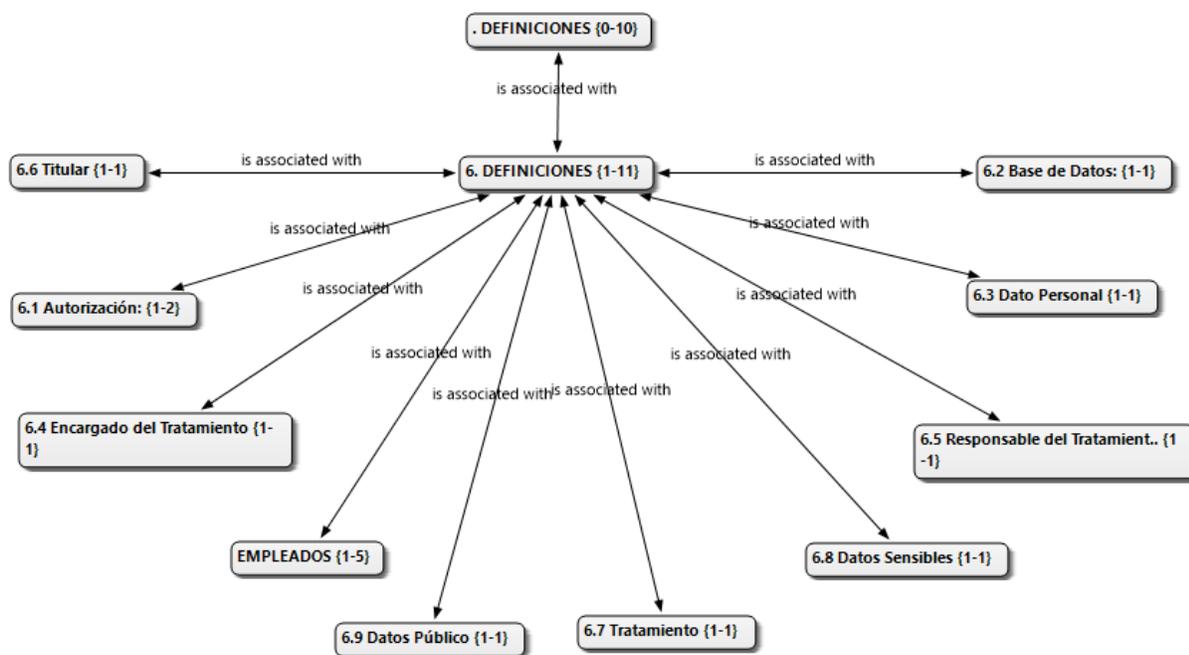


Figura 5. Definiciones de conceptos clave. Fuente: Construcción propia.

Luego de revisar los textos de las políticas de tratamiento de datos personales de las Universidades acreditadas de Bogotá se encuentra:

1. Todas las políticas cumplen con los elementos esenciales establecidos en el artículo 13 del Decreto 1377 de 2013. Lo que implica que están ajustadas a un marco normativo general, que responde al tratamiento de datos personales.
2. La finalidad de las políticas, está directamente relacionada con las tres funciones sustantivas de la universidades, es decir docencia, investigación y extensión (proyección social); la última, tiene que ver con la transferencia de conocimiento y el impacto generado por las universidades en el sector externo mediante la realización de convenios, la prestación de servicios, la educación continua, la oferta de diplomados, empleabilidad y el seguimiento a graduados, para lo cual, es necesario tener como referente, las finalidades establecidas en el registro nacional de bases de datos o los grupos de interés con los cuales tienen relación dado que, el uso continuo de dichas bases de datos, debe estar sujeto siempre a la política y de tratamiento de datos.
3. En cuanto a las calidades de los titulares, las IES tomadas como referente para esta investigación, realizan tratamiento de datos personales de menores de edad y principalmente de menores entre los 14 y los 17 años, solo cuatro de las políticas de tratamiento reconocen que realizan el tratamiento sin necesidad de la autorización de sus padres atendiendo al interés superior del menor estas IES son: Pontificia Universidad Javeriana (2017), Universidad Santo Tomás (2017) Universidad Colegio Mayor de Nuestra Señora del Rosario (2018) y EAN Universidad (2019).
4. Lo relacionado con los procedimientos para consultas y reclamos, en todas las IES que hacen parte de esta investigación, se realiza una remisión expresa a los términos legales

establecidos y se menciona los canales de atención y no se hace referencia una persona o área responsable.

Si bien cada una de las instituciones es autónoma para determinar el área responsable del proceso, es decir, no se evidencia al interior de la institución como se deben gestionar estas peticiones

El tratamiento de datos como ya se ha demostrado a través de la literatura consultada, es esencialmente en información básica de la persona y que muestra aspectos identitarios; así mismo, para la IES, se convierte un recurso no solo de conocimiento del estudiante, sino que es una herramienta que aporta a la consolidación de los sistemas de información y de obtener información relevante de la comunidad universitaria. En este sentido, y con el fin de analizar varios elementos se puede evidenciar que todas las universidades consultadas, cuentan con una política de tratamiento de datos, que reposa y puede ser consultada en el sitio web; otro elemento que comparten, es que los lineamientos son similares en cuanto al contenido propiamente dicho.

5. Las IES consultadas cumplieron con el deber de realizar el registro de sus bases de datos ante la superintendencia de industria y comercio, lo cual es un precedente importante, por cuanto el inventario de las bases de datos es un insumo importante para el establecimiento y desarrollo de un programa integral de protección de datos personales.
6. En cuanto al desarrollo de la responsabilidad demostrada en las políticas de las Universidades Acreditadas de Bogotá dos de ellas cuentan con Manuales Internos, publicados que se convierten en la hoja de ruta y en los que se encuentra claramente definida y expresa la declaración de dar cumplimiento.

En el siguiente cuadro se muestra las IES consultadas, que expresamente, consagran el principio de Responsabilidad demostradas en la política y/o en un manual interno:

Nombre Institución	Principio de Responsabilidad Demostrada
COLEGIO MAYOR DE NUESTRA SEÑORA DEL ROSARIO	Cuenta con Manual Interno
FUNDACION UNIVERSIDAD DE BOGOTA - JORGE TADEO LOZANO	No se evidencia en el texto
PONTIFICIA UNIVERSIDAD JAVERIANA	Cuenta con Manual Interno
UNIVERSIDAD ANTONIO NARIÑO	No se evidencia en el texto
UNIVERSIDAD CATOLICA DE COLOMBIA	No se evidencia en el texto
UNIVERSIDAD CENTRAL	No se evidencia en el texto
UNIVERSIDAD DE LOS ANDES	No se evidencia en el texto
UNIVERSIDAD DE SAN BUENAVENTURA	No se evidencia en el texto
UNIVERSIDAD DISTRITAL-FRANCISCO JOSE DE CALDAS	No se evidencia en el texto
UNIVERSIDAD EAN	No se evidencia en el texto
UNIVERSIDAD EL BOSQUE	No se evidencia en el texto
UNIVERSIDAD EXTERNADO DE COLOMBIA	No se evidencia en el texto
UNIVERSIDAD LIBRE	No se evidencia en el texto
UNIVERSIDAD MILITAR-NUEVA GRANADA	No se evidencia en el texto
UNIVERSIDAD NACIONAL DE COLOMBIA	Que el Decreto Reglamentario 1377 de 2013, con el fin de facilitar la implementación y cumplimiento de la Ley Estatutaria 1581 de 2012, reglamentó aspectos relacionados con la autorización del Titular de información para el tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias y transmisiones de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales.
UNIVERSIDAD PEDAGOGICA NACIONAL	No se evidencia en el texto
UNIVERSIDAD SANTO TOMAS	No se evidencia en el texto
UNIVERSIDAD SERGIO ARBOLEDA	No se evidencia en el texto

Figura 6. Políticas o manuales de protección de datos personales en IES – Colombia. Fuente: Construcción propia

Para esto, la Universidad Javeriana, en el Manual de Procedimientos de Protección de datos personales de 2017, por el cual se desarrolla la política de protección de datos personales; en el Numeral 8 establece:

Acreditación del principio de la responsabilidad demostrada (“ACCOUNTABILITY”) y el relacionamiento con terceros:

Para llevar a cabo un adecuado tratamiento de los datos personales, el Oficial de Protección de Datos Personales deberá validar los siguientes elementos de manera periódica:

- a) Revisión de las actividades que generan algún tipo de tratamiento de los datos personales
- b) Validación de los puntos de captura de información personal,

identificando el tipo de información que se recolecta y sus finalidades. c) Inventario y actualización de las bases de datos identificadas. d) Seguimiento al cumplimiento de las medidas de seguridad de las bases de datos y repositorios de información que se encuentren en el inventario.” (Universidad Pontificia Javeriana, 2017)

También, la Pontificia Universidad Javeriana, cuenta con los mecanismos para acreditar el cumplimiento del principio de responsabilidad demostrada y desarrollar en los demás numerales los elementos establecidos en la guía de responsabilidad demostrada de la Superintendencia de Industria y comercio (SIC).

La Pontificia Universidad Javeriana, cuenta con el cargo de Oficial de protección de datos personales, que depende directamente de la secretaria general que se encuentra adscrita a la Rectoría y cuya finalidad es demostrar el compromiso de la alta dirección con la protección de los derechos de los titulares de los datos.

Al interior de la Pontificia Universidad Javeriana se cuenta además con un Comité de Habeas Data de carácter interdisciplinar y personal encargado de las bases de datos que registra ante la SIC, en la fecha de consulta se pudo obtener el dato de 54 bases de datos registradas⁴. Que significa una toma de acciones necesarias para el tratamiento de bases de datos.

Tiene lineamientos adecuados para el uso de imágenes, datos biométricos y datos sensibles, incluso incluye el estudio de impacto como un mecanismo preventivo para garantizar la protección de los datos personales en el desarrollo de actividades y proyectos con terceros.

⁴ Tomado de: <https://www.sic.gov.co/registro-nacional-de-bases-de-datos>

Otro ejemplo, la Universidad del Rosario (2018), en el análisis al documento “Manual Interno para el tratamiento de datos”; se puede evidenciar donde se consagra expresamente el principio de responsabilidad demostrada:

Principio de responsabilidad demostrada: La Universidad está en capacidad de demostrar ante la Superintendencia de Industria y Comercio que ha implementado las obligaciones exigidas por la legislación colombiana en protección de datos personales atendiendo a su naturaleza jurídica, los servicios que ofrece a la comunidad académica y al público en general, estableciendo políticas, procedimientos, manuales, estructura de gobierno, inventario de las bases de datos, identificación de los riesgos asociados al manejo de datos y, en general, el cumplimiento de las obligaciones establecidas en la ley. (Universidad del Rosario, 2018).

En cuanto a lo establecido se puede inferir que el manual de la Universidad de Rosario es, aporta mayor claridad al desarrollar el principio de responsabilidad demostrada de forma detallada, con rigurosidad y de manera exhaustiva, muestra también los procedimientos que deben seguir los empleados de la universidad, durante todo el ciclo de datos y consagrando especiales lineamientos para los datos sensibles.

Respecto de la revisión de las políticas de las IES, se puede considerar que las universidades consultadas en la ciudad de Bogotá (Universidad de los Andes, 2013; Universidad Externado de Colombia, 2013; Universidad Pontificia Javeriana, 2017; Universidad Santo Tomás, 2017; Universidad del Rosario, 2018; Universidad Colegio Mayor de Nuestra Señora del Rosario, 2018; Universidad Nacional de Colombia, 2019), entre otras han adoptado este modelo en sus políticas de tratamiento de datos y en que puede exponerse de manera general: lo siguiente

- Los sujetos que se enmarcan en el tratamiento de datos personales.
- Los conceptos básicos y sus definiciones.
- Los principios jurídicos.
- Los derechos reconocidos por la ley.
- Urgencias y excepciones.
- Obligaciones de uso.
- Controles de seguridad.

Conclusión

En congruencia con lo expuesto, abordar el cumplimiento del Principio de Responsabilidad Demostrada en la política de protección de datos personales al interior de las Universidades Acreditadas de alta calidad en Bogotá-Colombia, da a lugar a la aproximación de las leyes y decretos que enmarcan el desarrollo del derecho en sí mismo. En este sentido, entender la importancia de la recolección de datos personales para el ámbito de Educación Superior, supone comprender que estos se encuentran inherentemente ligados a medidas de seguridad que deben en todo caso evitar la pérdida de la información.

Por tanto, luego de realizar el seguimiento a las universidades anteriormente expuestas, se hace evidente algunos puntos de convergencia como lo es el ajuste al marco normativo legal sobre la política de protección de datos personales y la estipulación de canales de atención. No obstante, se aprecia además algunas divergencias frente al uso del término Principio de Responsabilidad Demostrada que bien podría apelar a la falta de seguimiento sobre los desarrollos jurídicos y normativos.

CAPÍTULO TERCERO: Propuesta contenido mínimo para el diseño de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada.

Tabla 4

Encuadre de capítulo

Pregunta	¿Cuál es el contenido mínimo de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada en las universidades acreditadas de alta calidad en Bogotá Colombia?
Objetivo	Establecer el contenido mínimo para el diseño de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada para su comprensión y aplicación, acorde con las actividades misionales de las universidades acreditadas de alta calidad en Bogotá Colombia.

Fuente: Construcción propia

Para realizar una propuesta contenido mínimo para el diseño de un manual interno de normas y lineamientos para cumplir con el principio de responsabilidad demostrada, es necesario reconocer los antecedentes internacionales y nacionales sobre el mismo y sobre la regulación de protección de datos personales en general, dado que, sobre ellos es que se fundamenta el principio de responsabilidad demostrada en Colombia, es decir, son la base para la comprensión, entendimiento y aplicación; una propuesta debe estar sujeta a los antecedentes más relevantes, porque son ellos los que en últimas nutren los procesos y procedimientos.

Para su logro, se muestran referencias importantes en torno a la legislación a nivel internacional, esto con el fin de mostrar antecedentes relevantes sobre el tema, su orden refiere a dar una visión global por lo que se parte de la Unión Europea, se toman referencias de España y

Alemania por tener referentes importantes, seguidamente se muestra Estados Unidos por ser un referente en América y por último Colombia para ampliar la comprensión y sustentar la importancia de la propuesta de contenido mínimo:

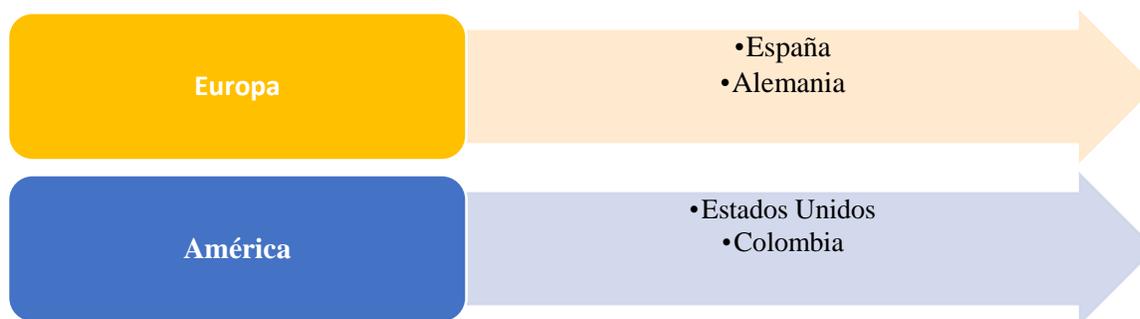


Figura 7. Referentes legislativos a nivel global. Fuente: Construcción propia

1. Europa

En cuanto a los desarrollos normativos en Europa, en el marco de identificar los aportes a nivel nacional e internacional de la política de protección de datos personales:

La protección de datos personales como un derecho fundamental fue firmado por 47 países en la Convención N° 108 del Council Europeo el 28 de enero de 1981, es legalmente el primer instrumento internacional de la Unión Europea que reconoce la protección de los individuos con respecto al procesamiento automático de sus datos personales (Martínez-Martínez, 2018). A esto, se añade el contenido del Artículo 8 de la Convención Europea de los Derechos Humanos. (ECHR, por sus siglas en inglés) (Consulado de Europa, 2010).

Se hace referencia también a los adelantos de la comisión europea, donde el uso de datos tiene una implicación en pilares fundamentales como la economía, la cultura, el estudio de mercados y en general tiene una influencia directamente proporcional con los recursos humanos y

financieros, este se convierte en un punto de partida y de análisis para establecer su impacto y aplicación:

Al respecto la Comisión Europea (2014), enuncia, cómo el buen uso y el tratamiento de datos aportan a la sociedad:

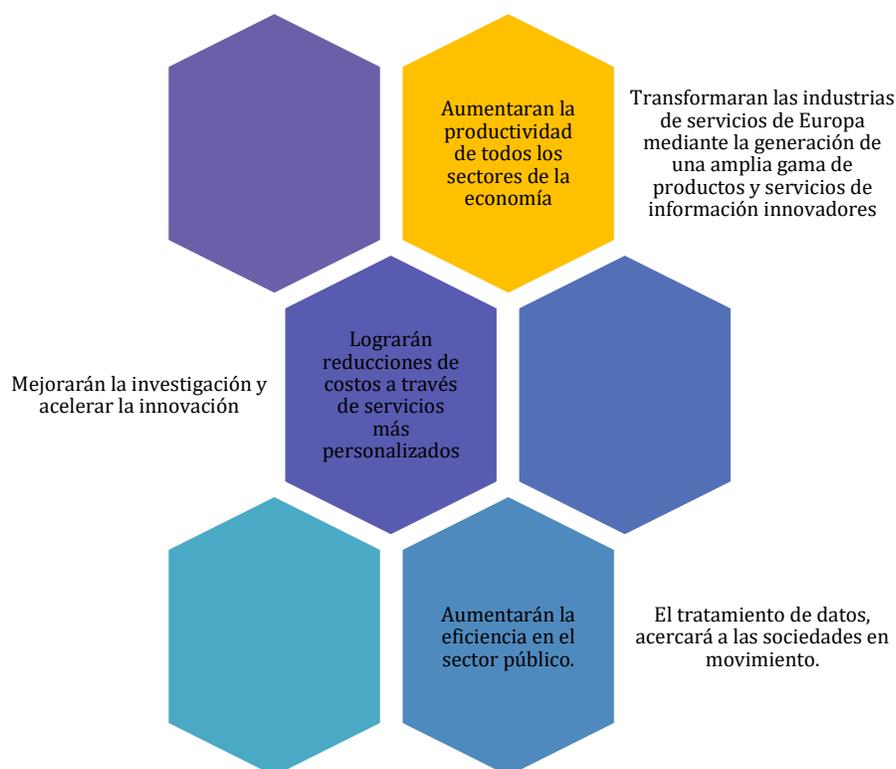


Figura 8. Aporte a la sociedad del buen uso y tratamiento de los datos. Fuente: Construcción propia recuperada de Monleón, 2015, p.p. 431-432.

La protección jurídica de los datos personales en el marco de la Unión Europea no constituye ninguna novedad. De hecho, son numerosas las referencias que encontramos en el derecho originario (artículo 6 del Tratado de la Unión Europea, modificado por el Tratado de Ámsterdam de 1997, y el artículo 286 introducido también por este último en el Tratado Constitutivo de la Comunidad Europea), el derecho derivado (o institucional), y la

jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. (Gutiérrez, s.f., p. 12).

El reglamento se expide, frente a la necesidad de actualizar la normativa de protección de datos personales del año 1995 que no preveía muchas de las situaciones que frente al uso de los datos, se genera con el acelerado desarrollo de la sociedad de la información y principalmente del creciente uso de internet para la prestación, oferta de servicios, y nuevas tendencias en el análisis de los consumidores, lo que incluye, , responsabilidad proactiva (demostrada) por parte del responsable del tratamiento, la inclusión de nuevas categorías de derechos como el derecho al olvido, el derecho a la portabilidad de los datos que habían sido desarrollados y reconocidos jurisprudencialmente.

El Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, y a través del cual se derogó la Directiva 95/46/CE, fue expedido en consideración a que el tratamiento de datos personales, en la Unión Europea, es un derecho fundamental.

Lo anterior coincide con la normatividad colombiana acerca del habeas data específicamente, el cual es consagrado como un derecho fundamental en la Constitución Política y que comienza a regir desde el 25 de mayo de 2018 (Gómez, 2019). De acuerdo con el RGPD:

(...) la protección que recibe este derecho fundamental, se garantiza sin distinción de la nacionalidad o residencia de las personas, y se fundamenta en la realización de un espacio de libertad, seguridad y justicia, sin dejar de lado el progreso económico y social de los mercados. Sobre el progreso de los mercados, el RGPD reconoce que los avances

tecnológicos y la economía digital, son los que impulsaron la expedición de una nueva reglamentación en materia de protección de datos, considerando al respecto que, en el marco de las nuevas tendencias en el manejo de la información, debe garantizarse la seguridad jurídica y práctica de los datos de las personas físicas, quienes deben tener control del tráfico de información que sobre ellas circula. (Gómez, 2019, p.18).

Para finalizar con este referente es importante mencionar: El reconocimiento de tres nuevos principios dentro del marco general, en especial del principio de responsabilidad que es reconocido de la siguiente manera en el artículo 5 numeral 2 del reglamento: “2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).” (Gómez, 2019).

1.1 España

En España, el derecho a la intimidad viene recogido en el artículo 18 de la Constitución, que acoge un contenido amplio de intimidad. Junto a la declaración general de positivización del derecho, se reconocen específicamente algunas facetas del mismo como la intimidad domiciliaria, la libertad y confidencialidad de las comunicaciones privadas o el secreto de las comunicaciones, para acabar con la constitucionalización del habeas data o faceta informática de la intimidad.

El derecho a la intimidad se recoge en la sección primera del capítulo II del título I de la CE⁵, donde se proclaman los derechos fundamentales. Ello conlleva que goce de las máximas garantías que el ordenamiento jurídico establece para dichos derechos. (Bru, 2007, p. 83)

⁵ Constitución Española.

Igualmente, para España, la agencia de protección de datos española, está facultada para la protección y el uso de los mismos en cualquier ámbito que se necesite.

En articulación con lo dicho anteriormente, Fernández (2012), realiza una reflexión que va más del tratamiento de datos y que refiere a su uso y alcance en la sociedad preguntándose por la información, por la privacidad el individuo y por la imagen, la reconstrucción de sí mismo, en fin, un debate sobre la identidad que no es ajena el discurso sobre el tratamiento de datos, dado que estos, son, en suma, elementos esenciales de la privacidad del individuo:

La posibilidad de mantener un control integral sobre los propios datos contribuye de manera determinante a definir la posición del individuo en la sociedad. No es casual que uno de los derechos consagrados en el art. 18 sea el derecho al honor (...) ¿qué es lo que debe percibir la sociedad? ¿La imagen que cada uno quiere dar de sí mismo? ¿La reconstrucción que otro puede ofrecer a partir de sus datos? En otras palabras, la atribución a un individuo del control sobre sus datos, ¿puede llevar a afirmar un derecho exclusivo de autorrepresentación? a estas preguntas cabe responder que el derecho a la autodeterminación informativa o libertad informática, no puede traducirse en un poder absoluto del individuo en las modalidades de composición y de representación de aquellas informaciones que son legítimamente disponibles a terceros. (Fernández, 2012, p. 129)

También, Fernández (2012), habla de la importancia de la privacidad y da alcance a la utilización de las bases de datos en España, que bien se puede aplicar a otros países y que son un elemento para garantizar que los individuos pertenezcan al sistema, y que se garanticen sus deberes y derechos, esto bajo el marco de protección a la privacidad.

1.2 Alemania

El segundo país que se trae a colación es Alemania, en donde se establece, el derecho a la autodeterminación informativa, como se explica:

El derecho a la autodeterminación informativa surge como respuesta a la posibilidad de un tratamiento masivo de datos. Fue construido y elaborado a partir de la sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983. En dicha sentencia, el Tribunal configura, a partir del derecho general de la personalidad recogido en el artículo 2.1 de la Ley Fundamental de Bonn, la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo, cuándo y dentro de qué límites, procede revelar situaciones referentes a la vida propia. Surge la necesidad de establecer jurídicamente mecanismos de protección de los datos personales frente a su uso informatizado, no tanto por el carácter estrictamente privado de éstos, sino por el peligro que supone la utilización que se haga de los mismos. En todo caso, el derecho no comporta una patrimonialización de los datos personales, sino que es la garantía de una serie de facultades individuales que permitirán al titular llevar a cabo el control y seguimiento de la información personal registrada en soportes informáticos. (Bru, 2007, p. 81)

2. América

2.1 Estados Unidos

Seguidamente se trae la visión de estados Unidos frente al tratamiento de datos y su implicación con la sociedad, alcance con los principios y valores propios de la condición humana y que se articulan con las del principio europeo, descrito anteriormente:

Con respecto al caso de EEUU, las derivaciones legales referentes a la protección de datos personales corresponden al principio europeo, si bien se carece de un organismo de control como en el caso de Europa, la disposición para su regulación gira en torno a las leyes sectoriales “El sistema jurídico anglosajón ha preferido promulgar normas sectoriales en materia de protección de datos personales. Se llama así a esta clase de leyes, porque son específicas para determinados sectores o materias. (Saltor, 2013, p. 276).

Estados Unidos separa la protección de datos por grupos poblacionales e instituciones, es decir, y como se muestra a continuación, la protección va dirigida en ejes diferentes para los niños y niñas en el sector educación, o bien para el uso de datos personales en entidades bancarias, expresamente en la Ley de Protección de la Intimidad de 1974 así:

La Ley de protección de datos del sector de la educación establece que tanto estudiantes como padres tienen derecho a acceder a la información captada desde este sector, y la comunicación de esta información sólo podrá ser comunicada a las instituciones públicas del país para usos administrativos, y a las autoridades en el manejo de supuestos legales. (Saltor, 2013, p. 277)

En general, el derecho a la protección de datos personales es un derecho a la intimidad, siendo así, las políticas creadas para la protección de datos es un poder para controlar el flujo de informaciones que conciernen a cada persona. (Pauner, 2015)

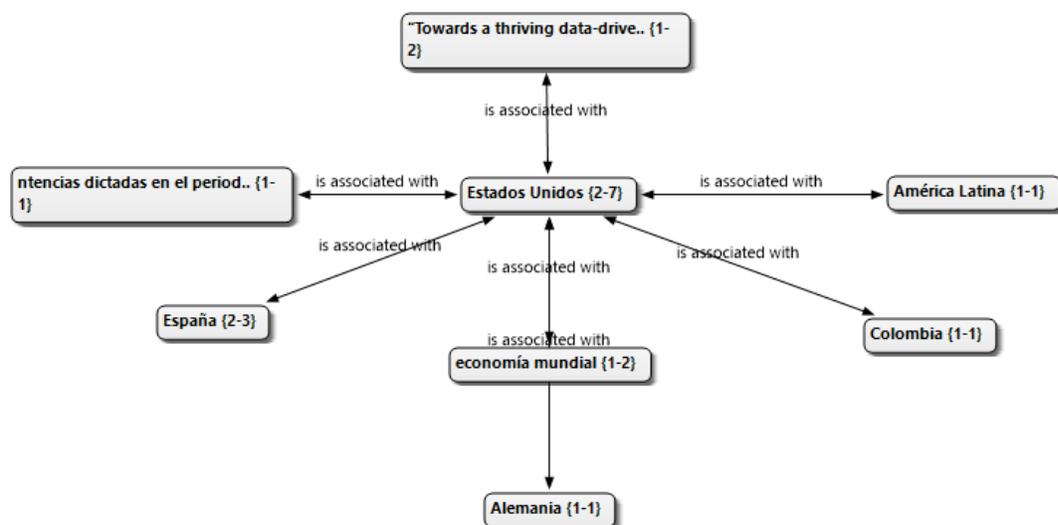


Figura 9. Hacia el uso de datos personales a nivel global. Fuente: Construcción propia.

La protección de datos personales se ha establecido desde las Constituciones Políticas. A continuación:

En una primera aproximación han sido dos países quienes han percibido los riesgos de la informática y por ello, incorporaron en sede normativa el reconocimiento de un derecho a la protección de datos personales. Por un lado, la Constitución Política de Perú establece “Toda persona tiene derecho (...) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. (García, 2007, p. 759)

3. Colombia

La Protección de datos personales en Colombia es un derecho fundamental consagrado en la Constitución Política de Colombia, en el Artículo 15, así:

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 los 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. (Esquema legal, 2019)

La citada norma fue desarrollada mediante la ley Estatutaria 1581 de 2012 y su reglamentación se encuentra compilada en el Decreto Único del sector de Comercio, Industria y Turismo número 1074 de 2015, así como por las circulares de la Superintendencia de Industria y Comercio SIC órgano que se encarga de la protección e inspección y vigilancia de la Protección de datos personales, mediante la Delegatura de Protección de Datos personales.

También, la perspectiva general de la regulación de protección de datos personales en Colombia y plantear las ventajas y los retos o desafíos que implica el implementar un programa de protección de datos personales desde una perspectiva de autorregulación, con una mirada ética del uso de los datos personales partiendo de la premisa de que más allá de la protección de los datos, quien es objeto de protección es el ser humano en su integridad y dignidad humana.

Así mismo, y con el ánimo de contribuir al relacionamiento con las leyes estatutarias, en Colombia se regula mediante el artículo 15 de la Constitución Política que establece dos leyes estatutarias: La ley 1266 de 2008 “que regula el derecho a la protección de datos personales frente a información financiera, crediticia, comercial, de servicios y la proveniente de terceros países” y la Ley 1581 de 2012 que regula el tratamiento de datos personales de manera general, se establecen los derechos, principios jurídicos.

Para Martínez, es necesario también hacer una reflexión consciente y coherente que contemple de forma integral a nivel nacional el tratamiento de datos, así mismo, su relación a nivel internacional:

“Así mismo, otro de los vacíos con los que cuenta la legislación colombiana es que está limitada y es insuficiente en el ámbito de aplicación territorial para la era digital, ya que no contempla el tratamiento de los datos personales en medios ubicados fuera del país.” (Martínez, 2019, p. 10).

Luego de mostrar la legislación más importante a nivel nacional e internacional en cuanto a la protección de datos y el principio de responsabilidad demostrada, con el fin que se comprenda que son un fundamento esencial para el diseño y la ejecución de norma en Colombia, y la importancia de este fundamento legislativo para dar una propuesta de contenido mínimo, dado que no es posible realizarla, sin tener claro los modelos, la legislación y la historia que se convierten en un soporte para su realización y comprensión.

En la primera ilustración se muestran los agentes y actores más relevantes para el tratamiento de datos que nutre su concepción de los antecedentes consultados, en la segunda ilustración se evidencia los contenidos mínimos para un manual de normas con el fin de cumplir con el principio de responsabilidad demostrada, allí se aclara que se realiza el ejercicio desde la mirada que del manual de la Universidad de Colegio Mayor de nuestra señora del Rosario, que se cita en la bibliografía y de la Pontificia Universidad Javeriana de Colombia, quien establece directamente en su recursos web un manual completo y de fácil consulta al usuario, en suma, es la compilación de elementos que pueden complementar la visión y de la Universidad para el tratamiento de datos.

Esta ilustración está directamente relacionada con los actores y agentes involucrados en el proceso de protección de datos:

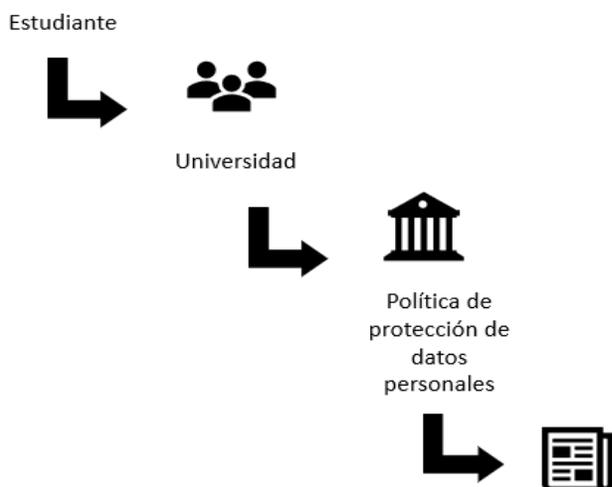


Figura 10. Agentes del proceso de protección de datos personales. Fuente: Construcción propia.

Precisamente, sobre estos actores se configura lo preponderante de reconocer el proceso por el cual se llega a la construcción del manual que permitiría a las IES el cumplimiento del Principio de Responsabilidad Demostrada.

4. Elementos y criterios comunes relevantes para la construcción de la propuesta

La propuesta tiene en cuenta la identificación de los grupos de interés de la IES que están explícitos casi en la mayoría de las políticas:

También, es importante nombrar que, de las IES consultadas, todas, tienen a definir una comunidad a la que está dirigida la política de seguridad de datos, es básicamente la comunidad universitaria:

1. Aspirantes.
2. Estudiantes.

3. Egresados.
4. Administrativos.
5. Personal docente.
6. Contratistas.
7. Terceros que participan en proyectos sociales que no tienen relación contractual con las IES.

Así, los datos personales que administran la Universidades, en cuanto a estudiantes y egresados, son los datos que tratan en virtud de una sola de sus funciones sustantivas, que es la formación de personas.

- **Comités de Ética**

En el desarrollo de las otras funciones sustantivas como la investigación y proyección social, administran un volumen de datos igual o similar que puede incluir el tratamiento de datos de menores de edad y de datos de salud, como en los comités de ética.

Los comités de ética son espacios que se propician dentro de la universidad, para el desarrollo de actividades que tienen que ver directamente con la protección de derechos de la comunidad universitaria en cuanto al diseño, ejecución y evaluación de proyectos de investigación, formación y creación e intercambio y circulación de conocimiento, este ente, también se encarga de orientar en principios éticos, derechos de autor y derechos patrimoniales, el comité es el ente que ubica el funcionamiento y el tratamiento de datos para los proyectos de investigación; según la normativa su función principal aportar al fortalecimiento de los aspectos éticos, dejar en claro los procedimientos para el tratamiento de los proyectos de investigación y contribuir al libre entendimiento de lo procedimental en lo investigativo. El comité de ética basa su proceder en “el

respeto de la dignidad humana, base de los principios que promueve la Declaración de Bioética y Derechos Humanos de la UNESCO:” El cual es un documento fundamental tanto para su diseño como para su ejecución:

La Conferencia General de la UNESCO adoptó, el día 19 de octubre de 2005, en París, la Declaración Universal sobre Bioética y Derechos Humanos. Esta Declaración propone la instauración internacional de principios comunes respecto a las cuestiones éticas relacionadas con la medicina, las ciencias de la vida y las tecnologías aplicadas a los seres humanos, teniendo en cuenta sus dimensiones sociales, jurídicas y ambientales.

(Universitat de Barcelona, 2006, p. 1)

Los comités de ética velan porque en las universidades se promueva de manera correcta y ética espacios y normativas claras frente a la cesión de derechos patrimoniales, morales y éticos cuando una comunidad académica promueve investigaciones de alto impacto y que están directamente ligados con aspectos de lo humano y su relación con los conocimientos científicos y tecnológicos:

La Declaración trata de propiciar nuevos enfoques de la responsabilidad social para garantizar que el progreso de la ciencia y la tecnología contribuyan a la justicia y la equidad y sirvan el interés de la humanidad. Así, la Declaración insiste en la necesidad de que los Estados cooperen en difundir la información científica y en estimular la libre circulación y el aprovechamiento compartido de los conocimientos científicos y tecnológicos. (Universitat de Barcelona, 2006, p. 1)

Así mismo, es importante mencionar los comités de bioética para el sector salud, que son los encargados, de discutir, promover y comprender los aspectos éticos directamente ligados a los

estadios de la vida humana, estos entes, que se articulan en las IES que cuentan con pregrados y postgrados del sector salud, propender por:

Los procedimientos que se establecen se orientan de manera prioritaria a la defensa de la seguridad, el bienestar y los derechos de los sujetos participantes, así como de la protección de otros seres vivos, involucrados en las investigaciones sobre las que influyen los Comités Institucionales de Ética en Investigación. Lo anterior de acuerdo con las orientaciones de las distintas declaraciones internacionales, especialmente de la Declaración de Helsinki y la Declaración Universal de Bioética y Derechos Humanos de la Unesco, así como de la normativa nacional vigente. (Velásquez, Ospina, Villegas, Robledo, Molina, Restrepo y Calle, 2015, p. 4)

Lo anterior se une a la discusión sobre realizar un análisis de las políticas y el desarrollo del principio de responsabilidad demostrada de las Universidades Acreditadas de Bogotá, dado que, dicho principio, está directamente ligado con el tratamiento y la utilización de datos. Está entonces establecido que las IES cuenten con un Comité de ética o bioética según sea el caso (en todas las áreas de conocimiento), su articulación con el principio de responsabilidad demostrada, busca en todo momento la correcta utilización y tratamiento con el tratamiento de datos en función de la producción de nuevo conocimiento y su divulgación y transferencia.

Es así que la realidad de los datos personales masivos es la de plantear la necesidad de un cambio de paradigma en lo que se refiere a la protección de datos personales y la privacidad que, en última instancia, requiere impulsar la adopción de normas robustas, claras y flexibles, en el sentido de adaptables, ya que fundamentalmente la falta de flexibilidad actual da lugar a situaciones de ineficiencia tanto al momento de aplicarlas como en lo relativo a su objetivo último, que es el de proteger a la persona titular de los datos personales. Esta finalidad, en

concreto, es a la que se referían hace ya más de un siglo Warren y Brandeis, al llamar la atención sobre la necesidad de dar el próximo paso para proteger a la persona a la vista de las “recientes invenciones y métodos de negocio” (Recio, 2017, p. 6)

La construcción de la propuesta se encuentra que todas las universidades comporten tres ejes en su objeto misional:

1. Docencia
2. Investigación
3. Servicio (extensión y proyección social) que implica relación con el entorno.

Las funciones sustantivas de las Universidades analizadas es muy importante comprenderlas por cuanto, son fundamentales para determinar el alcance del tratamiento de datos personales. En especial, lo relacionado con las actividades de investigación se deben articular adecuadamente con los lineamientos de los comités de investigación y ética y desarrollarse en el manual interno lineamientos claros de amonización de datos o establecerse una directriz. En cuanto al uso de imágenes, las Universidades realizan eventos académicos que son cubiertos por la oficina de comunicaciones o por las mismas facultades, cuentan con redes sociales, por lo que, es necesario que cuenten con unos lineamientos claros de uso de imágenes o mecanismos de amonificación que pueden ser implementados sin dejar de informar.

A continuación, se muestra el contenido mínimo de un manual de contenido mínimo para el principio de Responsabilidad Demostrada, en el cual se desarrollan de forma general, aspectos clave para su diseño e implementación:

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA



OBJETO

Establecer los lineamientos relevantes para la implementación del principio de responsabilidad demostrada y el tratamiento adecuado de datos personales.

ALCANCE

Los lineamientos planteados en el manual son de obligatorio cumplimiento para los empleados y encargados del tratamiento, deben aplicarse de acuerdo con el tratamiento de los datos, el alcance de la autorización otorgada por el titular y realizando un análisis mesurado cuando se contraponga la aplicación de otros derechos.

DEFINICIONES

El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular. (Ley 1581, 2012).

GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES

Oficial de protección de datos personales: Rol encargado de dar cuenta a la alta dirección, se recomienda que dependa de la secretaria general o del área de cumplimiento.
Comite de protección de datos personales: Conformado por un equipo interdisciplinar (seguridad informática, gestión documental, abogado, el oficial de protección de datos del nivel directivo.

IMPACTO CON TERCEROS

LINEAMIENTOS DE TRANSMISIÓN – TRANSFERENCIAS DE INFORMACIÓN DEL TITULAR TRANSFERENCIAS BANCARIAS HISTORIAS MEDICAS Y DOCUMENTOS DEL SECTOR SALUD.
TRANSFERENCIA SEGUN LAS ESPECIFICIDADES DE TRATADOS INTERNACIONALES
AUTORIZACION EN FORMATOS FISICOS
AUTORIZACION EN LA TOMA DE IMAGEN (VIDEO Y FOTOGRAFIAS)
AUTORIZACION PARA ACTIVIDADES PARTICULARES

INICIATIVAS QUE IMPLICAN EL IMPACTO DE PRIVACIDAD.

LINEAMIENTOS DE DATOS PERSONALES EN REDES SOCIALES, DATOS DE NAVEGACIÓN COOKIES Y WEB BUGS.

Administración del riesgo asociado al tratamiento de datos personales
Protección y seguridad asociada a los datos personales.

datospersonales@universidad.edu.co
www.universidad.edu.co

ACREDITACIÓN DEL PRINCIPIO DE LA RESPONSABILIDAD DEMOSTRADA (“ACCOUNTABILITY”) Y EL RELACIONAMIENTO CON TERCEROS

PROGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN
REVISIÓN Y ACTUALIZACIÓN DE BASES DE DATOS



INICIATIVAS QUE IMPLICAN EL TRATAMIENTO DE DATOS PERSONALES Y ANÁLISIS DE IMPACTO DE PRIVACIDAD

VERIFICACIÓN DEL CUMPLIMIENTO DE LAS DISPOSICIONES SOBRE DATOS PERSONALES

Procedimiento de atención a consultas y reclamos

datospersonales@universidad.edu.co



Figura 11. Fuente: Construcción propia.

Objeto: Diseñar el contenido mínimo de un manual que identifique los elementos relevantes del principio de responsabilidad demostrada empleados o encargados del tratamiento de datos personales de la Universidad los lineamientos y procedimientos internos para dar cumplimiento a la política de protección de datos personales bajo una óptica de responsabilidad demostrada.

Alcance: Los lineamientos planteados en el manual son de obligatorio cumplimiento para los empleados y encargados del tratamiento, deben aplicarse de acuerdo con el tratamiento de los datos, el alcance de la autorización otorgada por el titular y realizando un análisis mesurado cuando se contraponga la aplicación de otros derechos.

Definiciones.

Para efectos de la interpretación y aplicación de esta política deben tenerse en cuenta los siguientes conceptos:

a) Autorización: Consentimiento previo, inequívoco e informado del titular del dato para llevar a cabo el tratamiento de su información personal. (Ley 1581, 2012).

b) Autorizado: Persona autorizada por el titular de datos personales con el fin de que ésta efectúe en representación del titular cualquier tipo de trámite o solicitud ante la Universidad.

c) Base de Datos: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso. (Ley 1581, 2012).

d) Estudiante: Persona natural matriculada en algún Programa Académico ofrecido, tras cumplir los requisitos y procesos académico-administrativos exigidos.

e) Consulta: Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado.

El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular. (Ley 1581, 2012).

f) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ibídem).

g) Dato privado: Tienen como principal característica que pertenecen e interesan única y exclusivamente a la persona sobre la cual recae la información. (Recuperado 25 de agosto de 2017, Superintendencia de Industria y Comercio).

h) Dato público: Son los datos que no sean semiprivados, privados o sensibles. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377, 2013).

i) Dato semiprivado: Estos datos, aun cuando tienen el carácter de privado, sólo le interesan al titular y a un grupo determinado de personas, las cuales pueden consultar la información mediante una autorización. El ejemplo típico de esta clase de datos son las historias crediticias

que administran las centrales de riesgo. (Recuperado 25 de agosto de 2017, Superintendencia de Industria y Comercio).

j) Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Decreto 1377, 2013).

k) Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581, 2012).

m) Reclamo: El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento. (Ley 1581, 2012).

Responsable consultas y reclamos: Persona(s) que ha(n) sido designada(s) internamente por la Universidad para ejercer de manera formal la función de coordinar y gestionar las consultas y reclamos por datos personales que los titulares formulen.

o) Responsable del Tratamiento de la información: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581, 2012).

p) Titular del dato: Persona natural cuyos datos personales sean objeto de Tratamiento.

q) Trabajador: Es toda persona que en virtud de un contrato laboral se encuentra vinculado a la Universidad.

r) Trabajador administrativo: Es toda persona que en virtud de un contrato laboral se encuentra vinculado en cumplimiento de funciones administrativas.

s) Trabajador Docente: Es toda persona que en virtud de un contrato laboral se encuentra vinculado en cumplimiento de funciones académicas o relativas a la docencia.

t) Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país. (Decreto 1377, 2013).

u) Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable. (Ibídem).

v) Tratamiento de datos: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581, 2012).

w) Visitantes: Aquellas personas naturales que ingresan a las sedes y/o seccionales físicas.

- **En la autorización para toma de imágenes**

La finalidad de la anonimización es impedir que, a partir de una información o de una combinación de informaciones, se logren identificar sujetos individuales ya sean individuos, empresas o establecimientos, u otro tipo de unidades de observación en un archivo de microdatos (Morales, 2017: 5).

La Universidad debe verificar que la base de datos sea la versión más actual. En este caso, se recomienda que el periodo de tiempo del registro administrativo que se anonimizará, se defina con base en la periodicidad de consolidación de la información. Además, se recomienda revisar la consistencia y calidad de la base de datos teniendo en cuenta la sección Revisión de la consistencia de la base de datos de la Metodología de Diagnóstico de Registros Administrativos.

- **Gobierno en la protección de datos personales**

1. Oficial de protección de datos personales: Rol encargado de dar cuenta a la alta dirección, se recomienda que dependa de la secretaría general o del área de cumplimiento.
2. Comité de protección de datos personales: Conformado por un equipo interdisciplinar (seguridad informática, gestión documental, abogado, el oficial de protección de datos del nivel directivo)
3. Los administradores o responsables de las bases de datos que se registraron ante la SIC que son quienes deciden sobre las bases de datos.

- **Impacto con terceros**

Lineamientos de transmisión – transferencias:

Las universidades tendrán transferencias o transmisión de datos con los países que tengan clara el principio de responsabilidad demostrada y que se encuentren acorde a los lineamientos,

que cumplan de igual forma con los estándares establecidos por la Superintendencia de Industria y Comercio:

Información del titular

Transferencias bancarias

Historias médicas y documentos del sector salud.

Transferencia según las especificidades de tratados internacionales.

- **Iniciativas que implican el impacto de privacidad.**

Lineamientos de anonimización en casos específicos:

Imágenes personales: No se permite la identificación de los titulares, en los casos que la imagen no lo requiera, además, se debe tener en cuenta la autorización de la imagen por parte del titular.

- **Trabajos de grado-Investigaciones**

Todos los elementos que estén ligados al ámbito investigativo, se tendrá cuidado especial con el fin de respetar los derechos de autor, los derechos patrimoniales y morales, es decir, basado en normas internacionales que protejan tanto a al titular como a las universidades. También se pondrá especial atención en las citaciones y referencias con claridad, coherencia y citadas correctamente. El docente asesor se encargará en todos los casos de socializar a los estudiantes los parámetros, las condiciones y exponer con claridad la importancia de manejo adecuado de datos.

Es necesario recordar cómo se estableció anteriormente el papel preponderante del comité de ética de las universidades, para las investigaciones que estén directamente ligadas a su labor y conocimiento.

- **Lineamientos de datos personales en redes sociales, datos de navegación cookies y web bugs.**

En todos los casos es necesario contar con la autorización del titular, para la reproducción y uso de los datos. Cada instancia, como las direcciones de comunicaciones determina cuando se debe solicitar al titular la cesión de derechos correspondiente. Debe ser un procedimiento único y estándar delimitado por el sistema de calidad de la Universidad.

- **Administración del riesgo asociado al tratamiento de datos personales Protección y seguridad asociada a los datos personales.**

Lineamientos de bases de datos temporales, copias y reproducciones desarrollo y mantenimiento de sistemas: Sin importar su periodicidad y su uso, estas bases de datos deben de contar con el misma seguridad y autenticidad que las demás bases de datos. En todos los casos y cuando ya no se encuentren en uso, deben ser destruidas con las medidas de seguridad correspondientes, y lo más importante limitando u acceso y búsqueda de información. Sólo debe ser manipulada por personal autorizado.

Es necesario por parte de las facultades y unidades de apoyo, informar sobre la creación y el manejo de las bases de datos.

- **Redes en comunicaciones.**

Siempre debe tener como base y fundamento medidas de seguridad que van desde su utilización hasta el rol del encargado del manejo de la información, el personal de tecnología, debe de

comprender su rol, el uso y la importancia de la manipulación de la información de las bases de datos en cualquiera de los casos, asegurándose de su uso y transferencia.

- **Auditorías Internas**

En cualquiera de los casos, las auditorías internas, fijarán un procedimiento para el uso, la manipulación y la socialización de las bases de datos, articulada al sistema de calidad de la universidad y según su reglamento interno.

En cualquiera de los casos existirá un encargado de la socialización.

- **Generación de Cultura**

La universidad se encargará de divulgar a toda la comunidad académica sobre el uso y la importancia de presente manual y su contenido, de forma didáctica y pedagógica para que se comprenda y se asuma la importancia del manejo responsable de los datos personales suministrados y tratados.

- **Procedimiento de atención a consultas y reclamos**

El área responsable de garantizar los derechos del titular de los datos que consten en las bases de datos a cargo de la Universidad es la Secretaría General.

En el caso de que el titular considere que se ha dado un uso inapropiado, se han incumplido las finalidades antes descritas o se han desconocido los mandatos legales o sus derechos fundamentales, el procedimiento que debe seguir es el siguiente:

1. El titular del dato o su representante deberá presentar comunicación por escrito donde conste su calidad, informe su interés y exprese de manera clara los fundamentos de su solicitud.

2. La misma deberá ser radicada en la Secretaría General o a un correo electrónico, según sea el caso.
3. La Secretaría General procederá a dar respuesta en un término máximo de quince (15) días hábiles. En ella se señalará las medidas adoptadas con el fin de salvaguardar los derechos del titular.

- **Tratamiento y finalidades de las bases de datos**

La Universidades en su quehacer educativo lleva a cabo el tratamiento de datos personales de la persona titular que están contenidos y serán tratados en las bases de datos destinadas a finalidades legítimas, considerando la Constitución Política y la Ley 1581 de 2012. Los datos son tratados de manera lícita, leal y transparente conforme a las finalidades que el titular autorizó y son recolectados para brindar educación y orientación integral a los estudiantes (titulares), para el cumplimiento de aspectos jurídicos, contractuales y en general para el desarrollo de las actividades.

- **Tratamiento de datos en el marco de la Ley 1266 de 2008**

Las Universidades como fuente de información en el marco de tratamiento de datos relacionados con información de servicios, comercial, financiera y crediticia, solicitará a través del Administrador de la base de datos, el consentimiento para las consultas y reportes a centrales de riesgo de los Titulares de los datos registrados.

También, notificará al titular (en caso de que aplique) en el plazo legal vigente al Titular sobre la operación previamente a remitir información a las centrales de riesgo y cumplirá las obligaciones que señala la ley como fuente de información.

- **Personas facultadas por ley para solicitar información y/o ejercitar derechos**

Las universidades resolverán consultas o reclamos que presenten las siguientes personas facultadas por ley:

- Por el titular, su representante o tutor para el caso de menores de edad o ...
- Por sus causahabientes
- Por el representante y/o apoderado del titular
- Por estipulación a favor de otro y para otro

Tales personas pueden ejercer algún derecho con relación al tratamiento de los datos personales del titular acreditando la calidad según corresponda.

- **Anonimización de datos personales**

Las universidades garantizarán los derechos de los titulares, a que se respete su intimidad y privacidad, por tanto, adoptará procesos de anonimización de los datos personales.

La anonimización radica en delimitar y suprimir la información del titular que permita su identificación y considerando su solicitud de anonimato como condición para autorizar su tratamiento o publicación.

Se aplicará los procesos de anonimización para evitar la posible identificación de las personas para garantizar sus derechos. Para esto, la Universidad valorará las técnicas de anonimización previo a la publicación de datos personales, lo cual implica la responsabilidad de las personas encargados del tratamiento de datos, incluyendo los datos sensibles y menores de edad. Para esto es necesario la formación del personal a cargo para la implementación de medidas

de confidencialidad, uso de estándares y buenas prácticas que determinen una adecuada anonimización de datos personales.

Es importante considerar que para garantizar la anonimización, la Universidad debe considerar cierto grado de pérdida de utilidad, debido a que entre más datos se anonimicen, menor será la utilidad de los datos resultantes. La anonimización se logra al disociar los datos de tu titular. De lo anterior es importante aclarar que la Universidad realizará seguimientos periódicos con el fin de asegurar que los datos anonimizados permanezcan disociados de su titular.

Proceso de anonimización

- Equipo de trabajo: recurso humano proporcional al volumen del tratamiento de los datos y al proceso de anonimización, delegado del área jurídica, personal capacitado en protección de datos que evalúe los riesgos y destinatarios de la información anonimizada, un representante del área de Tecnologías de la Información que se encargue de las medidas de seguridad necesarias. Se debe determinar la calidad y funcionalidad de los datos, su proyección y su anonimización.
- Identificación de riesgos de reidentificación: Los proceso de anonimización no garantizan de manera absoluta la protección de los datos, sin embargo la Universidad debe verificar caso a caso para detectar y reducir posibles riesgos. En la identificación de los riesgos, el equipo de trabajo tendrá en cuenta las siguientes categorías:
 - a. Riesgos de reidentificación existentes conocidos
 - b. Riesgos potenciales de reidentificación
 - c. Riesgos no conocidos

Una vez identificados los riesgos se establecerán medidas encaminadas a minimizar el eventual impacto para la privacidad de las personas que pudieran ser reidentificadas, las cuales deberán ponerse en conocimiento del Administrador de la base de datos y el recurso humano con acceso a la información.

- **Preanonimización**

Se establece el objetivo de los datos que se propone anonimizar, para crear una lista de los datos necesarios para cumplir con dicho objetivo, al hacer esto se establecen los niveles de protección necesarios, la sensibilidad, su carácter de identificación y los datos que deben ser eliminados. Para esto se establecen las siguientes categorías de sensibilización y el riesgo de reidentificación:

1. Datos de identificación geográfica.
2. Datos de identificación directa de personas o **empresas**.
3. Datos con magnitudes numéricas.
4. Datos de carácter sensible
5. Datos sin restricción para el acceso al público.
6. Datos categóricos.

- **Seudoanonimización**

La seudoanonimización es hacer uso de identificadores ciegos con el fin de mantener la

concentración de los datos propios de un único individuo sin revelar su identidad.

- **Técnicas de anonimización**

La Universidad adoptará la técnica de anonimización que mejor se adapte al objetivo de los datos y al proceso de anonimización, para esto se deben considerar los análisis de riesgos y el uso de herramientas para proteger los datos y la privacidad de los titulares. Algunas técnicas de anonimización:

- Métodos de aleatorización o perturbación
 - Microagregación: Variables numéricas
 - Adición de ruido: útil cuando los atributos pueden causar un importante efecto adverso en las personas y consiste en la modificación de atributos mediante la generación de valores aleatorios
 - Permutación o intercambio de registros: intercambiar valores de un registro a otro
 - Redondeo: sustitución del valor de las variables originales por valores redondeados
- Métodos de reducción o generalización
 - Eliminación de variables
 - Eliminación de registros
 - Recodificación
 - Supresión de celdas
 - **Anonimización de datos personales en casos específicos**

La anonimización de datos no puede ser generalizada, se deben considerar las

particularidades propias de cada caso, su objetivo y el tipo de información que se debe anonimizar. Los datos serían los siguientes:

- Imágenes personales
- Investigaciones
- Tesis y trabajos de grado
- Videovigilancia.

Conclusión

De este modo, el manual propuesto, con todas las características que requiere como lo son su objetivo, el alcance, entre otros, posibilita que estudiantes y demás interesados tengan conocimiento previo acerca del manejo que se le va a dar a sus datos, los fines de su recolección, el anonimato que refiere y demás para evitar posteriores dificultades o conflicto de intereses, además posibilitar que sea de fácil acceso, visibilidad y comprensión. Esto también permite que tanto la entidad, en este caso una IES, y también el estudiante o interesado, lleguen a acuerdos frente al tratamiento que se les dará a los datos y de esta forma se aplique el principio de responsabilidad demostrada aplicado claramente en Colombia.

Conclusiones Finales

A lo sumo, el análisis realizado acerca de la aplicación del Principio de Responsabilidad Demostrada en las Universidades Acreditadas de alta calidad de Bogotá, refleja la forma en la que las instituciones listadas incorporan la protección de datos personales, los parámetros sobre los que se organizan para garantizar este derecho fundamental, que cobra especial importancia en la era actual, en donde la sociedad digital prima.

El recorrido normativo y el marco de aplicación a nivel mundial y nacional, son marcos generales sobre los que la propuesta parte para llegar ya localmente, a comprender los retos que a nivel de las IES se tiene para desarrollar el Principio de Responsabilidad Demostrada en la política de la protección de datos desde sus propias singularidades y procesos.

REFERENCIAS BIBLIOGRÁFICAS

- Azurmendi, A. (2018). Derechos digitales de los menores y datos masivos. Reglamento europeo de protección de datos de 2016 y la Coppa de Estados Unidos. *El profesional de la información*, 27(1), 27-35.
- Beltrán, J.C., Pineda, A.K. y Quevedo, A. (2016). *Análisis de los riesgos que causan la fuga de información en la empresa Asesorías Contables y Revisoría Fiscal JAA S.A.S.* (Tesis especialización). Universidad Católica de Colombia, Colombia.
- Blog Agencia Española de Protección de Datos Personales (25 de octubre de 2018). Riesgos a los que puede enfrentarse la labor del delegado de protección de datos, recuperado de www.aepd.es/blog .
- Bru, E. (2007). La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de Internet, Derecho y Política*, 5, 78-92.
- Chen, S. (2010). Privacidad y protección de datos: un análisis de legislación comparada. *Diálogos*, 11(1), 111-152.
- Congreso de Colombia. (28 de Diciembre de 1992). Ley 30. Servicio Pública de Educación Superior. Recuperado de: https://www.cna.gov.co/1741/articles-186370_ley_3092.pdf
- Congreso de Colombia. (2012). *Ley 1581. Régimen General de Protección de Datos*. Recuperado de: http://www.secretariassenado.gov.co/senado/basedoc/ley_1581_2012.html
- Consejo Nacional de Acreditación. (s.f.). Acreditación de programas de pregrado. Recuperado de: <https://www.cna.gov.co/1741/article-186377.html>

Congreso de Colombia. (1991). *Constitución Política de Colombia*.

Consulado de Europa. (2010). Convenio Europeo de Derechos Humanos. Recuperado de:

https://www.echr.coe.int/Documents/Convention_SPA.pdf

Corte Constitucional. (2011). Sentencia C-748. República de Colombia. Recuperado de:

<http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>

Cubero, J. y Aberasturi, U. (2008). Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la ley 25/2007, sobre conservación de datos. *Revista Española de Derecho Constitucional*, 83, 175-197.

Dirección Nacional de Escuelas (DINAE). (s.f.) Políticas de privacidad y condiciones de uso.

Recuperado de: <https://www.policia.gov.co/direcciones/educacion-policial>

Escuela de Administración de Negocios. (2019). Política de Tratamiento de Datos Personales.

Recuperado en:

<https://universidadean.edu.co/sites/default/files/institucion/acuerdos/politica-tratamiento-de-datos-personales.pdf>

Esquema Legal. (29 de agosto de 2019). *Derecho al buen nombre - la honra y habeas data*.

Recuperado de: http://esquemalegal.com/archivo/derechos/d_buen_nombre.php

Fernández, C. (2012). Algunos retos de la protección de datos en la sociedad del conocimiento.

Especial detenimiento en computación en nube (Cloud computing). *Revista de derecho*, 10, 125-145.

- Frigeiro, C. (2018). Mecanismos de regulación de datos personales: Una mirada desde el análisis económico del derecho. *Revista Chilena de Derecho y Tecnología*, 7(2), 45-80.
- Fuquene, E.D. (2019). Rol de la legislación colombiana en la evolución de la seguridad informática y de la información.
- García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, 120, 743-778.
- Gligora, M., Debeljak, Sandra & Kadoić, N. (2019). Preparing Students for the Era of the General Data Protection Regulation (GDPR). *TEM Journal*, 8(1),150-156.
- Gómez, A. (2019). *La aplicación extraterritorial del nuevo reglamento europeo de protección de datos personales y su incidencia en Colombia*. (Tesis de especialización). Pontificia Universidad Javeriana, Colombia.
- Guía para la protección de la privacidad y los frutos transfronterizos de datos personales (1980). OCDE.
- Gutiérrez, V. (s.f.). Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa. *Derecho y conocimiento*, 3, 1-19.
- Harroch R, Martin J,y Smith R. V. (11 de noviembre de 2018). Forber. San Francisco, EU.; Data Privacy and Cibersecurity Issues in Mergers And Acquisitions. Recuperado de: <https://www.allbusiness.com/data-privacy-cybersecurity-issues-mergers-and-acquisitions-due-diligence-checklist-119265-1.html>
- Hernández, E. y Zavala, O. (2018). Datos personales en las relaciones laborales del sector privado. *Revista Latinoamericana de Derecho Social*, 27, 221-231.

- Jefatura del Estado. (05 de diciembre del 2018). Ley Orgánica 3. Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado. Recuperado en:
<https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf>
- Maqueo, M.; Moreno, J. y Recio M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho*, 30(1), 77-96.
- Martínez, A. (2019). La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *Revista la Propiedad Inmaterial*, 27, 5-23.
- Martínez-Martínez, D. (2018). Unificación de la protección de datos personales en la unión europea: desafíos e implicaciones. *El profesional de la información*, 27(1), 185-194.
- Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 5, 47-61.
- Minero, G. (2014). A vueltas con el "derecho al olvido" construcción normativa y jurisprudencia del derecho de protección de datos de carácter personal en el entorno digital. *RJUAM*, 30(2), 129-155.
- Ministerio de Comercio, Industria y Turismo. (2013). Decreto N° 1377. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Recuperado de:
<http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf>
- Ministerio de Comercio, Industria y Turismo. (2015). Decreto N° 1074. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Recuperado de:

<http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201074%20DEL%2026%20DE%20MAYO%20DE%202015.pdf>

Monleón, A. (2015). El impacto del Big-data en la Sociedad de la Información. Significado y utilidad. *Historia y comunicación social*, 20(2), 427-445.

Monsalve V. (2017). La protección de datos de carácter personal en los contratos electrónicos en consumidores; análisis de la legislación colombiana y de los principales referentes europeos.

Naciones Unidas. (2015). *Declaración Universal de Derechos Humanos*. Recuperado de: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

Ojo al dato. (10 de julio de 2017). Nueva Ley Federal de Protección de Datos en Alemania (BDSG). Recuperado en: <http://ojoaldatolegal.com/nueva-lopd-en-alemania>

Parlamento Europeo y del Consejo. (2016). Reglamento General de Protección de Datos Personales. *Diario Oficial de la Unión Europea*. Recuperado en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Pauner, C. (2015). La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística. UNED, *Teoría y Realidad Constitucional*, 36, 377-395.

Pérez, A. (2009). La protección de los datos personales del menor en internet. Anuario Facultad de Derecho - Universidad de Alcalá, 2, 143-175.

Pouillet, Y. y Dinant, J. (2007). Hacia nuevos principios de protección de datos en un nuevo entorno TIC. *Revista de Internet, Derecho y Política*, 5, 33-46.

- Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. *Revista de Derecho Civil*, 5(4), 53-87.
- Recio, M. (2017). Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas. *Revista de derecho común*, 17, 4-25.
- Remolina, N. (2015). *Recolección Internacional de Datos personales: un reto del mundo post – internet*. Agencias Española de Protección de Datos Personales.
- Remolina, N. y Álvarez, L.F. (2018). Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.
- República Bolivariana de Venezuela. (2009). Constitución de la República Bolivariana de Venezuela. Recuperado en: http://www.sudebip.gob.ve/wp-content/uploads/2018/05/Constituci%C3%B3n-RBV_con-enmienda-de-2009.pdf
- Rodríguez-López, M. (2012). “Códigos tipo: derecho a la información y protección de datos personales”. *El profesional de la información*, 21(5), 509-513.
- Roig, A. (2009). E-privacidad y redes sociales. *Revista de los estudios de derecho y ciencia política de la UOC*, 9, 42-52.
- Román F, (mayo 2018), Preservar la Privacidad en la era Digital, FORBES México, recuperado www.forbes.com.mx .

Saltor, E. (2013). *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina* (Tesis Doctoral). Universidad Complutense de Madrid, España.

Sanz, F. (2015). Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. *Revista luz et Praxis*, 22(1), 323-376.

Sentencia de Constitucionalidad C -748, (2011), Corte Constitucional de la Republica de Colombia, recuperado www.corteconstitucional.gov.co.

Sistema Nacional de Información de Educación Superior. (s.f.). *Búsqueda de Instituciones de Educación Superior*. Recuperado de:
<https://snies.mineduacion.gov.co/consultasnies/institucion#>

Superintendencia de Industria y Comercio (SIC). (27 de mayo de 2015). *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)*. Recuperado de: <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

Superintendencia de Industria y Comercio. (s.f.). Sobre la protección de datos personales. Recuperado de: <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *Revista de Internet, Derecho y Política*, 13, 53-66.

Troncoso, A. (2009). Reutilización de información pública y protección de datos personales. *Revista General de Información y Documentación*, 19, 243-264.

Universidad de los Andes. (2013). Manual de políticas de tratamiento de datos personales.

Recuperado de: <https://uniandes.edu.co/>

Universidad Nacional de Colombia. (2019). Política de tratamiento de datos personales.

Recuperado de: <http://unal.edu.co/>

Universidad Santo Tomás. (2017). Política de tratamiento de la información personal.

Recuperado de: <https://www.usta.edu.co/>

Universidad Colegio Mayor de Nuestra Señora del Rosario. (2018). Política de tratamiento de datos personales de la Universidad del Rosario. Recuperado de:

<https://www.urosario.edu.co/>

Universidad Pontificia Javeriana. (2017). Manual de políticas de tratamiento de información y protección de los datos personales. Recuperado de: <https://www.javeriana.edu.co/home>

Universidad Pontificia Javeriana. (2019). MANUAL DE PROCEDIMIENTOS DE

PROTECCIÓN DE DATOS PERSONALES. Recuperado de:

<https://www.javeriana.edu.co/documents/15832/0/Manual+de+Procedimientos+de+Protecci%C3%B3n+de+Datos+Personales/e9cb83e8-2728-4ee2-ae20-e76bc4d886a5>

Universidad Externado de Colombia. (2013). Política de tratamiento de datos personales.

Recuperado de: <https://www.uexternado.edu.co>

Universitat de Barcelona. (2006). La Declaración Universal sobre Bioética y Derechos Humanos adoptada por la UNESCO. *Revista de Bioética y Derecho*, 6, 1-2. Recuperado de:

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/RevBioDerecho_Mar06.pdf

Varela, C. y Ameneiros, R. (2018). La protección de datos personales en las bibliotecas universitarias españolas en el entorno digital. *Revista General de Información y Documentación*, 28(2), 685-702.

Velásquez, JP.; Ospina, D.; Villegas, EM.; Robledo, SM.; Molina, ME.; Restrepo JG. y Calle, JI. (2015). Manual para el funcionamiento de los Comités de Ética en Investigación de la Universidad de Antioquia. Universidad de Antioquia. Recuperado de:
<http://www.udea.edu.co/wps/wcm/connect/udea/d583fef0-dab7-485b-811b-7e4fc4088489/manual-comites-etica.pdf?MOD=AJPERES>

Vergara, M. (2017). Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. *Revista Chilena de Derecho y Tecnología*, 6(2), pp. 135-152