Hoja de Ruta
Cumplimiento ley 1581 de 2012
de protección de datos personales

UNIVERSIDAD DEL QUINDÍO

Elaborado por:	Revisado por:	Aprobado por:
José E. García Castro	**Martha C. Sánchez**	**John E. Martínez García**
Consultor	Gerente del Proyecto	Consultor Senior

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
0.0	27/09/2017	Emitido para aprobación
1.0	29/09/2017	Revisado
2.0	30/09/2017	Aprobado

Contenido

1 HOJA DE RUTA

Con el fin de generar un ambiente de entendimiento de la normatividad de protección de datos personales por parte de la Universidad del Quindío y, con el objetivo de atender los lineamientos y mejores prácticas para que al momento de la creación o gestión de las bases de datos personales, la Universidad cumpla la normatividad aplicable con base en las mejores prácticas, se ha elabora la presente hoja de ruta para unificar criterios respecto del tratamiento de datos personales que servirá como guía para cumplir con los requerimiento legales y garantizar el respeto de los derechos titulares.

La aplicación de la presente Hoja de Ruta parte de la tipología de datos que administra la Universidad, así como del proceso de diagnóstico que se realizó para evaluar el cumplimiento de la Ley 1581 de 2012 y la aplicación de buenas prácticas en protección de datos.

2 MARCO NORMATIVO A TENER EN CUENTA

El artículo 15 de la Constitución Política, en el capítulo de Derechos Fundamentales, consagra los derechos de todas las personas a conservar su intimidad, mantener su buen nombre y a la protección y garantía de su derecho al Habeas Data. Teniendo en cuenta estos aspectos, la protección de la privacidad de los datos personales se encuentra íntimamente relacionada con el derecho a la intimidad y al buen nombre.

Con el fin de desarrollar el derecho al Habeas Data, se han incorporado al ordenamiento jurídico colombiano distintas normas que propenden por la buena administración de la información personal, comercial y financiera de los titulares, dentro de las cuales se encuentran la Ley 1266 de 2008, la Ley 1581 de 2011 y el Decreto 1377 de 2013.

La Ley 1581 de 2011 y el Decreto 1377 de 2013

No obstante fueron implementados y reglamentados los impulsos legislativos ya mencionados, se hacía necesario aún que se estableciera un sistema robusto de

protección que otorgue a los Titulares de la Información mecanismos precisos para salvaguardar sus derechos ante los Responsables o Encargados del tratamiento de los datos personales, planteando, también, la posibilidad de acudir a la Autoridad de Control. Por esta razón, siguiendo los principios planteados en las anteriores normativas, se expide la Ley 1581 de 2012 que surge como una complementación de la Ley 1266 de 2008, norma esta última que se refiere a un ámbito muy preciso de datos y responde a particulares necesidades de los usuarios del sector financiero que es necesario conservar, y cuyo carácter limitado impone la necesidad de regular el universo de los tipos de datos no cobijados por la Ley 1266 de 2008.

Como ámbito de aplicación, el artículo 2º de la Ley 1581 de 2012 establece con claridad que ***"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por Universidades de naturaleza pública o privada…",*** situación que impone la necesidad de que las Universidades estatales, de cualquier nivel, observen lo allí establecido y adecúen su actividad a los principios, deberes y responsabilidades dispuestos por la citada Ley.

En ese sentido, la Ley 1581 de 2012 regula el derecho al Habeas Data, especialmente en lo referente al derecho a conocer, actualizar, y rectificar información contenida en bases de datos o archivos, conforme a lo establecido en el artículo 15 y 20 de la Constitución Política de Colombia.

La Ley 1581 de 2012, define el marco general o los parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo, entre los cuales se encuentran los principios de legalidad, finalidad, libertad, transparencia, seguridad, confidencialidad, garantía de veracidad y calidad de la información y límites en el acceso y circulación restringida en materia de tratamiento de datos.

De esa manera, la Ley ha fijado los límites frente a las actividades de responsables y encargados del tratamiento de la información que permitirán garantizar los derechos de los titulares de los mismos, propugnando que los datos sean adquiridos, tratados y manejados de manera lícita, garantizando que el tratamiento de la información de los ciudadanos - titulares obedezca a una finalidad legítima de

acuerdo con la Constitución y la Ley y que sólo pueda ejercerse con el consentimiento, previo, expreso e informado del titular.

Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento, el cual es además, calificado, por cuanto debe ser previo, expreso e informado. Por ello, el silencio del Titular nunca podría inferirse como autorización del uso de su información, por lo que el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez.

Así, como principio esencial, el tratamiento de la información sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley.

Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido. Por ello, se debe evitar que los datos privados, semiprivados, reservados o secretos puedan estar junto con los datos públicos, y por tanto, los primeros no pueden ser objeto de publicación en línea, a menos que se ofrezcan todos los requerimientos técnicos y se debe eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación a los datos personales del titular.

Asimismo, el marco normativo aplicable requiere que la información sujeta a tratamiento por las Universidades del Estado, y también por Universidades privadas, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, garantizando la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente Ley y en los términos de la misma.

Con ocasión en lo anterior, se establece como regla general la prohibición de someter a tratamiento los datos sensibles, salvo algunas excepciones a dicha regla, en las que el tratamiento de tales datos es indispensable para la adecuada prestación de servicios –como la atención médica y la educación- o para la

realización de derechos ligados precisamente a la esfera íntima de las personas – como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión.

Promulgada la Ley 1581 de 2012, se expide por el Gobierno Nacional el Decreto 1377 de 2013, cuya finalidad, entre otras, es facilitar la implementación y cumplimiento de la Ley 1581 de 2012, reglamentando aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, los contenidos mínimos de las políticas de Tratamiento de los Responsables y Encargados, la forma en que se garantiza el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y el desarrollo del principio de responsabilidad demostrada frente al tratamiento de datos personales.

En virtud de lo establecido por el Decreto 1377 de 2013, además de ser necesario contar con la autorización para realizar el tratamiento de los datos personales, la cual debe otorgarse a más tardar en el momento en que se realice la recolección de los datos a ser tratados, debe observarse la figura de las Políticas de Tratamiento, documento que debe hacerse disponible en medio físico o electrónico, escrito de manera clara y sencilla para su compresión, con el objeto de informar al Titular sobre el tratamiento que se le dará a los datos y la finalidad para la cual es tratado el mismo.

De la misma manera, en tal política deberán constar los derechos de los titulares, así como la persona o área responsable del Tratamiento de los datos personales, ante la cual se pueden ejercer los derechos legales y presentar las reclamaciones relacionadas con el derecho al Hábeas Data, y el procedimiento o las maneras para ejercerlos.

Por otra parte, el Decreto 1377 de 2013 señala que los responsables del tratamiento de datos personales deben estar en capacidad de demostrar[1], a petición de la Superintendencia de Industria y Comercio, Autoridad única en materia de Protección de Datos, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones que la Ley les impone, proporcionales a la naturaleza jurídica de la organización empresarial responsable del mismo.

[1] Artículo 26. 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.

Entre tales medidas se encuentran la obligación de conservar la copia de la respectiva autorización otorgada por el Titular de manera tal que se pueda verificar con posterioridad, conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento e informar, a solicitud del Titular, sobre el uso dado a sus datos. Asimismo, resaltamos, como elemento integrante de las medidas apropiadas, el deber de los Responsables de informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la Ley y en el Decreto 1377 de 2013.

3 DEFINICIONES A TENER EN CUENTA

Con el fin de lograr entendimiento a los pasos y recomendaciones plasmadas en la Hoja de Ruta, es necesario se tengan en cuenta las siguientes definiciones determinadas en el Artículo 3° de la Ley 1581 de 2012. Definiciones. Para los efectos de la presente ley, se entiende por:

a. **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

b. **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento;

c. **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

d. **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;

e. **Responsable del Tratamiento:** 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;

f. **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento;

g. **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Para ampliar las definiciones, tenemos:

a. **Aviso de Privacidad:** Mecanismo subsidiario de comunicación, verbal o escrita, generada por el Responsable, acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales. El Aviso de Privacidad será, entonces, la forma de informar a los titulares sobre la existencia de las políticas de tratamiento cuando no sea posible ponerlas a disposición de los titulares, deber que debe cumplirse a más tardar “al momento de la recolección de los datos personales.”

b. **Base de datos:** Se entiende por base de datos o banco de datos, a un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, por tanto incluye desde bases de datos de personal, empresas de servicios, contratistas y candidatos hasta sistemas robustos de información.

c. **Contratos de Transmisión de Datos:** El Artículo 25 del Decreto 1377 de 2013 lo define como el contrato que suscriba el Responsable con los Encargados para el tratamiento de datos personales bajo su control y responsabilidad, señalando los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el responsable.

d. **Cookie**: Es un archivo que envía un servidor web al disco duro del internauta que lo visita, con información sobre sus preferencias y sobre sus pautas de navegación a la hora de ingresar a internet.

e. **Datos de tráfico:** Son los datos de comunicación relativos a las actividades en las redes públicas, en los que se incluye información relativa al origen de la comunicación, el destino de la misma, la fecha, la hora, el contenido de la comunicación, el destino y su duración, entre otros.

f. **Datos públicos:** Se catalogan como datos públicos todos aquellos que no son de naturaleza semiprivada o privada, como también los contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva, y los relativos al estado civil de las personas. Entre los datos de naturaleza pública a resaltar se encuentran: los registros civiles de nacimiento, matrimonio y defunción, y las cédulas de ciudadanía apreciadas de manera individual y sin estar vinculadas a otro tipo de información.

g. **Datos personales:** La clasificación de datos personales, hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Se engloban dentro de esta clasificación todos los datos tratados dentro de las Hojas de Registro, como por ejemplo datos sensibles, datos de la salud, datos laborales, etc.

h. **Datos sensibles:** El artículo 5º de la Ley 1851 de 2012 señala que “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.”. Los datos de naturaleza sensible deben ser asimilados como una tipología de datos personales.

i. **Encargado del Tratamiento:** La Ley 1581 de 2012 define al Encargado del Tratamiento como aquella “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.” En otras palabras, el Encargado es quien realiza el tratamiento de datos personales en virtud de la delegación o mandato por parte del Responsable. Entre dichos encargos se encuentran la obtención de

autorizaciones por parte de los ciudadanos y la verificación de cumplimiento de la finalidad en la recolección por parte de la Universidad.

j. **Entes fiscalizadores:** Entidades que en ejercicio de sus funciones legales pueden solicitar lícitamente a otras Universidades los datos personales que obren en sus bases de datos, tales como la Fiscalía General de la Nación, Contraloría General de la República, Unidad de Información y Análisis Financiero, etc.

k. **Función legal:** Potestad otorgada por el ordenamiento jurídico a la Universidad para poder realizar el tratamiento.

l. **Información privada:** Información que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones, así como por decisión del titular de los mismos. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

m. **Información reservada o secreta:** Información que por su estrecha relación con los derechos fundamentales del titular, como su dignidad, intimidad y libertad, se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida ni siquiera por autoridad judicial en el cumplimiento de sus funciones. Cabe mencionar la información genética, y los llamados "datos sensibles", como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación, o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.

n. **Información semi-privada:** La información que presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las Universidades de la seguridad social o de los datos relativos al comportamiento financiero de los ciudadanos

o. **Mecanismos de defensa de perímetro:** Son los mecanismos relacionados con firewalls, sistemas detección de intrusos, sistemas de prevención, software anti-virus/anti-spyware.

p. **Mecanismos de PQR´s:** Los mecanismos atinentes a que los titulares conozcan, actualicen, rectifiquen y supriman sus datos personales, se refieren concretamente a procedimientos eficientes de Peticiones, Quejas y Reclamos. Esto quiere decir, mecanismos de atención al titular con los que cuenten las Universidades, para que los Titulares de la Información puedan presentar solicitudes de petición, quejas o reclamos respecto a sus datos personales.

q. **Políticas de Tratamiento:** Documento disponible en medio físico o electrónico, escrito de manera clara y sencilla para asegurar su compresión, con el objeto de informar al Titular sobre el tratamiento que se le dará a los datos y la finalidad para la cual es tratado el dato. De la misma manera, en tal política deberán constar los derechos de los titulares, así como la persona o área responsable del Tratamiento de los datos personales, ante la cual se pueden ejercer los derechos legales y presentar las reclamaciones relacionadas con el derecho al Hábeas Data, y el procedimiento o las maneras para ejercerlos. En la política de tratamiento deben constar, de manera clara, la forma de ejercer, por parte del titular de la información, el derecho a revocar la autorización otorgada para el tratamiento, así como los procedimientos para ejercer el derecho a conocer, actualizar, rectificar, y suprimir el dato.

r. **Políticas internas efectivas:** Documento cuyo objetivo tiende a demostrar, ante un requerimiento de la Superintendencia de Industria y Comercio, autoridad nacional en materia de protección de datos personales, la existencia de una estructura administrativa proporcional a la estructura y tamaño de la Universidad, así como la adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento, programas de educación y procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento, así como la implementación efectiva de las medidas de seguridad apropiadas, que demuestre de manera efectiva el cumplimiento de sus deberes como responsable del tratamiento.

s. **Responsable del Tratamiento:** Siguiendo lo dispuesto por la Ley 1581 de 2012, y el Decreto 1377 de 2013, se denomina Responsable del Tratamiento a toda persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, tenga poder de decisión sobre las bases de datos y/o el Tratamiento de los datos, entendiendo por tratamiento "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión". El Responsable define, entonces, la forma en que se almacenan, recolectan y administran tales datos, definiendo, también, los fines esenciales para los cuales se realiza el tratamiento. Asimismo, está obligado a solicitar y conservar la autorización en la que conste el consentimiento expreso del titular de la información, así como a mantenerlo informado, con suficiencia y claridad, acerca de las finalidades específicas del tratamiento mismo.

t. **Root-kits:** Programas típicamente clandestinos y maliciosos que permiten un acceso constante y privilegiado a un equipo de manera oculta del control de los administradores. Corrompe el funcionamiento normal del sistema operativo y de otras aplicaciones. Se utiliza para esconder algunas aplicaciones que podrían actuar en el trasfondo sistema atacado.

4 LA CREACIÓN O IDENTIFICACION DE LAS BASE DE DATOS

Paso N° 1: Identificar la función legal de la Universidad

Como primer paso, y con el fin de aproximar la Universidad a los principios básicos del manejo de información personal proveniente de la población estudiantil, empleados, terceros en general, que de ahora en adelante y según la definición, serán los titulares, es preciso anotar que la administración de los datos personales empieza desde antes de que se comience a recolectar la información de los titulares.

Obligación legal	La determinación de la función que la Ley le ha otorgado. De esta manera, la función legal ejercida por la Universidad, a la hora de realizar cualquier tratamiento sobre datos personales es crucial, puesto que todo tratamiento debe estar definido a una facultad otorgada por el ordenamiento que autorice su finalidad.
Mejores prácticas	En ese sentido, antes de iniciar la recolección de cualquier tipo de información y de crear o identificar una determinada base de datos, se recomienda que la Universidad realice las siguientes actividades: ✓ La Universidad debe, primero, identificar cuál es la disposición normativa que la habilita para recolectar los datos personales que busca recopilar. Para ello la Universidad debe buscar la disposición expresa en la Ley que la habilite para ello, y tomar nota de las expresiones de la misma. ✓ Una vez se precisada la norma habilitante, esta debe tenerse muy en cuenta a lo largo del proceso, toda vez que podrá ser consultada posteriormente. ✓ Luego, debe analizarse la norma y consultar si en ella se estipula algún procedimiento especial para la

		obtención, almacenamiento y utilización de la información.

Paso N° 2: Definir la necesidad y la finalidad en la recolección:

Teniendo clara la función que ha sido otorgada por la Ley a la Universidad para adelantar las acciones de cara al titular, es necesario tener claro el objetivo de la recolección de la información que se pretende recolectar[2].

El artículo 4º de la Ley 1581 de 2012 trae a colación el principio de finalidad, por el cual se entiende que el tratamiento de datos debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley y que ésta finalidad debe ser informada al titular, quien debe otorgar una autorización, un consentimiento previo, expreso e informado para llevar a cabo el tratamiento de los datos personales.

Esta finalidad legitima los procesos de administración de la información a recopilar.

Con base en lo anterior, la Universidad debe definir el porqué de la recolección. Para ello debe realizarse un ejercicio interno en virtud del cual la Universidad debe:

- ✓ Realizar un listado de objetivos. Estos serán los fines para los cuales recolectará la información.
- ✓ Precisar qué datos se requieren para cumplir tales objetivos.
- ✓ Realizar un cuidadoso examen acerca de la sensibilidad de los mismos, señalando si estos constituyen información semi-privada, privada, reservada o secreta, sensible, o pública, según las definiciones propuestas al inicio de esta hoja de ruta.
- ✓ Definir a cuál de las finalidades enlistadas se adecúa, procediendo a agruparla información que considera necesaria, dependiendo de la finalidad del tratamiento de los datos personales.

[2] Artículo 4. Ley 1581 de 2012. Numeral b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

En resumen, la Universidad debe partir de la identificación de su función legal para así contrastar dichas funciones con el propósito y los motivos por los cuales se realizará la recolección de los datos.

La finalidad para la recolección de información delimitará el uso que se dará a los datos recabados. Es decir, la Universidad no podrá realizar el tratamiento de la información con una finalidad distinta a aquella que se determine como objetivo para la recolección de los datos personales. Esto, salvo que medien razones de innovación, desarrollo, ciencia o estadística, así como políticas estatales que favorezcan a toda la población.

Paso N° 3: Identificar el límite temporal para el manejo de la información

La finalidad escogida definirá también el factor de tiempo durante el cual se adelantará el tratamiento de los datos personales, pues, según lo requiere la Ley 1581 de 2012, el tratamiento de la información debe realizarse por un periodo acorde a la finalidad y necesidad planteada o determinada en la paso N° 2.

Se debe detallar de manera clara, cuál será el periodo de tiempo razonable al cabo del cual se agotará la finalidad para la cual se recolectó la información.

Debe anotarse que no se requiere establecer un número determinado de días, meses o años, pero sí es considerada una buena práctica hacer referencia a circunstancias o condiciones que marquen el agotamiento de la finalidad identificada.

Paso N° 4: Identificar a los titulares de la información

La Universidad debe conocer y determinar la población que va a brindar sus datos para las finalidades ya identificadas. Con esta actividad se podrá saber quiénes van a aportar sus datos personales y qué tipo de datos alimentarán las bases de la Universidad.

Esto permitirá a la Universidad definir a su vez, si la finalidad para la cual se recopila la información genera algún tipo de beneficio para los titulares, siendo entonces necesario que se detallen estos beneficios, así como las situaciones adversas que pueden derivarse de los mismos.

La Universidad debe tener claridad acerca de la posibilidad de generar perfiles de los titulares, a partir de la información recolectada.

Los beneficios detallados, que deben ser informados a los titulares, pueden ser exigidos por éstos, al paso que deben también conocer las situaciones adversas o la posibilidad de que se les incorpore en un grupo determinado de personas que cumplen características comunes.

Así, si existen ciertos requisitos, parámetros, calidades o situaciones objetivas verificables para determinar si deben recabarse datos de un titular específico, la Universidad debe elaborar una lista de chequeo acerca de tales características, el cual servirá para evitar obtener información innecesaria.

Para estos fines, la Universidad debe tener en cuenta que los titulares que en el futuro exijan ser parte de una base de datos no podrá negarse injustificadamente el ingreso a las plataformas de información. En otras palabras, a estos titulares se les debe garantizar su derecho a consultar la información entregada.

De acuerdo a la Ley 1581 de 2012, el titular tiene el derecho de comprobar que los datos que circulen sobre él han sido previamente autorizados, solicitar prueba de ello y revocar su autorización, conocer, actualizar y rectificar sus datos personales en los casos en que estos sean inexactos, incompletos o fraccionados, que induzcan a error o cuyo tratamiento se encuentre prohibido.

- ✓ Recordar que ell titular tiene derecho a exigir que su información sea tratada de conformidad con los límites impuestos por la Ley y la Constitución, y que en caso de incumplimiento, existe un recurso efectivo para lograr el restablecimiento de sus derechos.

Paso N° 5: Designar al Responsable y Encargado de las bases de datos

La Universidad debe elegir al servidor público o Macroproceso Responsable de administrar las bases de datos que se van a crear.

- ✓ ***Se debe diferenciar entre Responsable y Encargado del Tratamiento***

La selección del personal responsable debe realizarse atendiendo a la idoneidad y a las competencias necesarias para adelantar la labor, para que de esta manera se escojan los servidores públicos mejor capacitados en el manejo de información.

Para tales fines, la Universidad debe:

- ✓ Evaluar las competencias de cada uno de ellos.
- ✓ Evaluar la experiencia de los servidores públicos de cara a la tarea que van a realizar.
- ✓ Evaluar el conocimiento en materia de seguridad de la información, con el fin de escoger los servidores públicos que, a futuro, tengan las capacidades suficientes para atender incidentes de esta índole.

Independiente de la naturaleza del responsable (individual o colectivo) la Universidad debe crear un régimen de responsabilidades acorde con las funciones de los servidores públicos designados como responsables, así como un reglamento que consagre las consecuencias de la mala administración de la información.

Adicionalmente se debe tener en cuenta, que en la Universidad, los servidores públicos pertenecientes al área de salud, bienestar universitario, Manejo de Población Vulnerable y Actividades de Investigación en Salud y que están encargadas de administrar los datos personales relacionados con datos de salud, la Universidad deberá indicarles a estos servidores que deben suscribir un acuerdo de confidencialidad sobre los datos personales de esta naturaleza, indicándole además las consecuencias por incumplirlo.

- ✓ ***Esto adicional a las resoluciones emitidas por la Rectoría en materia de Código de Ética y Buen Gobierno.***

La Universidad debe asegurarse de comunicarle a los servidores públicos al momento de conferirle la función, la existencia de dichos regímenes de responsabilidades y de sanciones aplicables.

Paso N° 6: Formular la Política de Tratamiento de Datos Personales

Para la correcta administración de datos personales, la Universidad debe elaborar la Política de Tratamiento de Datos Personales, en cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013, con el fin de que en esta se definan los aspectos esenciales aplicables a la administración de ellos.

De esta manera se debe proceder a elaborar un documento que contenga como mínimo los siguientes elementos:

- ✓ Nombre, razón social, domicilio, dirección, correo electrónico y teléfono del Responsable y del Encargado de las bases de datos personales.
- ✓ Derechos de los titulares de la información.
- ✓ Servidor público o área responsable de atender las Peticiones, Quejas y Reclamos que se presenten ante la Universidad.
- ✓ Fecha de su entrada en vigencia.
- ✓ Los servidores públicos que tendrán acceso a las bases de datos.
- ✓ El uso de contraseñas y procedimientos de autenticación de quien está autorizado a consultar las bases de datos.

Datos de la salud: Si se trata de datos reservados, los servidores públicos designados para la administración de estos datos, no podrán en ningún momento transferir ni delegar esta función, por lo que la Universidad deberá velar porque ello no ocurra.

Datos laborales: Si los datos a recolectar son susceptibles de crear perfiles acerca de la población, deberá garantizar que la información que pueda ser usada para actos discriminatorios, sea conocida únicamente por los servidores públicos autorizados para dicho fin, garantizando además, que solamente ciertos servidores públicos de la Universidad tengan acceso a ella. Por este motivo, la Universidad deberá garantizar que los servidores públicos que tendrán acceso a estas bases de

datos será un grupo bastante pequeño en comparación a quienes tendrán acceso a otros tipos de datos.

En la formulación de la Política, además de incluir los aspectos generales anteriormente mencionados, debe incluirse también un aparte dedicado al Responsable y Encargado de las bases de datos, en la cual se indique la identificación de estos servidores públicos y las obligaciones y funciones que deben desempeñar.

Cuando la Universidad haya definido estos aspectos esenciales de la Política de Tratamiento, se debe proceder a elaborar un Folleto Informativo que será dirigido a todos los titulares, en donde se explique cuál es la función legal de la Universidad, la finalidad que busca con la recolección de los datos personales y la necesidad de recopilarlos.

Este Folleto Informativo debe ser redactado en un lenguaje claro para que cualquier titular lo entienda.

- ✓ **Recordar que la Política de Tratamiento tiene una naturaleza cambiante, en donde es permitido modificar e incluir apartes dentro de esta cada vez que sea necesario.**

Conformación del Comité Consultivo

La Universidad en marco del cumplimiento de lo dispuesto en la Ley 1581, debería conformar un Comité consultivo el cual estará encargado de cumplir funciones consultivas en favor de la Universidad en cuanto a la protección de datos personales.

Este Comité debe ser conformado por los servidores públicos que están mejor informados o por su función manejan los temas de protección de datos personales, el Responsable y Encargado de la información, los miembros que en cada macroproceso son responsables de la administración de los datos personales y los servidores públicos o sus delegados que dentro de la Universidad se estime

conveniente incluir, por ejemplo, Macroproceso de Gestión Documental, Gestión de Apoyo Académico, Control Interno, Gestión de Tics, Gestión Jurídica, entre otros.

Para efectos de la convocatoria, la Universidad deberá identificar, primero, a los sujetos llamados a conformarlo, atendiendo los servidores anteriormente mencionados, para que en las situaciones que prevé esta Hoja de Ruta y en los casos en los que la Universidad lo considere conveniente, sean convocados al Comité y citados a la mesa de trabajo que se debe adelantar, indicando además, la fecha, hora y lugar en la que sesionará y los temas que serán tratados en la reunión.

- ✓ **Este comité será el órgano colegiado interno de carácter consultivo que podrá ser convocado cuando la Universidad así lo requiera.**

Paso N° 7: Elaborar el Reglamento de Seguridad de la Universidad

Después de definir la Política de Tratamiento, se formula la Política de Seguridad para la administración de datos personales, la cual, siendo igual de significativa que la anterior política, permite diseñar las medidas de seguridad para la salvaguarda de los datos personales, de cara a los riesgos inherentes a la administración de este tipo de información.

De esta manera, la Universidad debe preparar las plataformas físicas en las cuales reposara la información, ya sea los computadores y equipos de hardware dedicados al almacenamiento de los datos personales, y los programas y demás aplicaciones –software- que garanticen un proceso exitoso en la recolección, manejo y cancelación de la información.

Antes de elaborar las medidas de seguridad, se deberá:

- ✓ Destinar los recursos técnicos y de talento humano especializados para implementar las medidas de seguridad necesarias para mantener la integridad de los datos personales de los titulares.
- ✓ Capacitar constantemente a los servidores públicos involucrados en la labor, acerca de los riesgos a los que se pueden enfrentar los datos personales, implementando sesiones de capacitación para ello.

Definidos estos aspectos se procede a elaborar las políticas de seguridad en la que se logre identificar los miembros de la gestión, quienes serán los autorizados para consultar internamente la información, restringiendo el acceso a los servidores que no están habilitados para ello.

La Universidad debe organizar sus sistemas de información para recopilar los datos, siempre formulando estas políticas de acuerdo a la naturaleza de los datos que se van a recopilar y la forma como estos van a ser consultados.

Partiendo de la Planeación Estratégica de TI y Análisis de Riesgos de la Universidad, se deben definir los niveles de seguridad en los van a ser clasificados los datos recolectados, dependiendo de la naturaleza de los mismos y de los riesgos a los que estarán expuestos:

Nivel básico de seguridad para las bases que administran una cantidad baja de datos personales, como también para aquellas que manejan datos que no tienen la calidad de reservados, privados o sensibles.
Nivel medio de seguridad para las bases de datos que administran un número considerable de datos y para aquellas que manejen datos que tengan un nivel de privacidad moderado y no se cataloguen dentro de los niveles de seguridad básico o alto.
Nivel alto de seguridad para las bases que administran gran cantidad de datos, como también para aquellas que manejan datos de naturaleza reservada, privada o sensible.

Datos laborales Si los datos personales del titular permiten conocer la identificación y la ubicación de una persona con una afiliación sindical en particular, los niveles de seguridad aplicables serán los de clasificación media o alta, pero nunca básica.

Datos reservados Si la naturaleza de los datos a administrar es de naturaleza reservada, el nivel de seguridad aplicable debe ser el más riguroso y no podrá ser inferior al nivel alto de seguridad.

Se debe tener presente que la motivación y la justificación que generó la clasificación de las bases de datos en distintos niveles de seguridad o en un nivel

especifico, deben estar consignadas dentro de un documento elaborado por los Responsables de la información.

La Universidad debe implementar medidas de seguridad para la administración de los datos personales, tales como contraseñas de acceso a la información, tarjetas de seguridad, puertas cerradas para acceder a las plataformas físicas, almacenamiento de la información de manera cifrada o codificada y en general cualquier medida que sea considerada conveniente para restringir el acceso a la información y al lugar donde esta se encuentre.

Desde el macroproceso de Gestión de TICs, se deben tomar las medidas de seguridad determinando los siguientes aspectos:

- ✓ Protocolos de seguridad dedicados a dar respuesta a las fallas de seguridad del sistema.
- ✓ Descripción de los recursos protegidos.
- ✓ Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido para cada base de datos.
- ✓ Descripción de los sistemas de información aplicados en el proceso de seguridad.

Además de definir los elementos de salvaguardia de la integridad de los datos personales, se tenga en cuenta que durante la administración de la información pueden ocurrir hechos que vulneren los datos almacenados, por lo que es necesario que se definan los procedimientos para la gestión de incidentes, los cuales deben estar diseñados con el fin de contener y recuperar los datos perdidos ante una falla, identificar a quienes es necesario notificar ante el suceso e investigar y dar respuesta a los incidentes.

Como ya existe un trabajo en la identificación de los riesgos, se debe reforzar la identificación de los riesgos a los que se pueden ver expuestas las bases de datos y diseñar los protocolos especiales para la mitigación del riesgo o actuación ante la ocurrencia de uno de ellos, con el fin de que si ocurre un suceso negativo, las políticas de seguridad tengan predispuestos los procesos de contención y recuperación, y las medidas para evaluar los acontecimientos y generar políticas para prevenirlos en el futuro.

Estas políticas deben contener además, un registro de sucesos en el que se plasmen todos los acontecimientos que ocurran en relación con la base de datos.

El responsable y/o Encargado debe elaborar un informe periódico que indique:

- ✓ Los acontecimientos del sistema.
- ✓ El rendimiento de los sistemas de seguridad.
- ✓ Los problemas que se han presentado.
- ✓ Las soluciones ideadas a las fallas.

Cuando se logren definir todos los aspectos anteriormente descritos, las políticas de seguridad formuladas conformarán el Reglamento de Seguridad de la Universidad, el cual debe ser construido antes de la recolección de los datos personales de los titulares y ser incluido dentro de la Política de Tratamiento de Datos Personales.

Paso N° 8: Capacitación de los servidores públicos

Luego de definida la Política de Tratamiento de Datos Personales e incluirse en esta el
Reglamento de Seguridad de la Universidad, los servidores públicos que van a ser involucrados en la recolección de los datos, deben ser capacitados con respecto a estas políticas, sin olvidar por supuesto que entre los módulos de aprendizaje se debe incluir además, el régimen sancionatorio aplicable ante un incumplimiento y un módulo dedicado exclusivamente al Código de Ética de la Universidad.

Es importante que al finalizar cada uno de los módulos, se evalúe el conocimiento adquirido por los servidores públicos en las capacitaciones realizadas.

Para todo lo anterior, deberá destinarse el tiempo adecuado para transmitir al servidor los conocimientos necesarios para administrar la información, sin olvidar que esto puede ser sujeto a evaluaciones periódicas que midan el conocimiento de los servidores públicos encargados.

Datos estadísticos y poblacionales: Para la administración de datos de naturaleza estadística y poblacional, la Universidad deberá capacitar al personal encargado del tratamiento, con el fin de brindarles los conocimientos necesarios para identificar los riesgos que se puedan generar para la seguridad pública del Estado o de la Universidad.

Paso N° 9: Definir la Política de Trazabilidad e Interoperabilidad de Datos Personales

Si en marco de las funciones legales de la Universidad, se ejecuten procesos o actividades que ameriten la transferencia de datos entre Universidades Privadas o Universidades del Gobierno, es necesario que antes de administrar los datos personales, se encuentren definidas las políticas que respondan a este tipo de situaciones.

Esta Política especial debe contener los protocolos de seguridad dedicados a los procesos de trazabilidad e interoperabilidad que eviten la ocurrencia de riesgos tales como la adulteración, perdida, consulta, uso o acceso no autorizado de los datos, o implementación fraudulenta de los mismos.

El Responsable y Encargado de las bases de datos se encuentra en la obligación de identificar los riesgos que existen en el proceso de interoperabilidad o trazabilidad entre Universidades o Universidades del Gobierno, y estableciendo actividades de la seguridad de la información, deben formularse igualmente protocolos especiales de seguridad ante la ocurrencia de un riesgo, estos, dirigidos a mitigar y reparar el daño causado en el transcurso de estos procesos o actividades.

Paso N° 10: Elaborar el Aviso de Privacidad y la Autorización dirigida al titular

Antes de iniciar la recolección de los datos personales por parte de la Universidad, es necesario que se creen los documentos de Aviso de Privacidad y de Autorización, los cuales serán entregados y suscritos respectivamente al titular de la información.

El Aviso de Privacidad tiene la finalidad de comunicar al titular de la información acerca de las Políticas de Tratamiento que componen la administración de sus datos, la cual debe incluir como mínimo, según el artículo 15 del Decreto 1377 de 2013, lo siguiente:

- ✓ Nombre o razón social y datos de contacto del responsable del tratamiento.
- ✓ El tratamiento de los datos y la finalidad de la recolección.
- ✓ Los derechos del titular.
- ✓ Los mecanismos dispuestos por el Responsable para que el titular conozca la Política de Tratamiento de la Información y los cambios sustanciales que se puedan producir en ella.

Debe indicarse también la dependencia de la Universidad, los servidores públicos que tendrán acceso a sus datos y la razón que los habilita para ello, así como la información que le permita al titular ejercer sus derechos.

Por último y con respecto al Aviso de Privacidad, para dar cumplimiento a la normatividad pertinente, la Universidad debe planificar de qué forma los titulares pueden consultar los cambios en la Política de Tratamiento de los datos personales en el futuro y comunicarla al titular.

Deberá entonces informar acerca de los mecanismos ya sea vía Página Web de la Universidad[3], personalmente en las instalaciones de la Universidad, telefónicamente por medio de una línea de atención (call-center), o la que se considere más conveniente, pero siempre respetando este derecho del titular.

La Autorización del ciudadano permite que éste al ser debidamente informado acerca de la administración de sus datos personales, pueda consentir de manera libre, previa y expresa la recopilación de estos.

Por estos motivos, al momento de recopilar los datos del titular, se debe informar a este acerca de la finalidad y la necesidad que tiene la Universidad en la labor legal y misional y obtener la autorización del titular antes de usar sus datos.

[3] http://www.uniquindio.edu.co/

Si durante la recopilación de los datos personales, necesariamente se tiene que involucrar a un menor de edad o a un incapaz (según las disposiciones establecidas en el Código Civil) debe surtirse un procedimiento especial para conseguir su autorización, toda vez que debe contarse con la debida participación de su representante.

Si al recolectar los datos de un titular, necesariamente debe involucrarse la información de un tercero, se debe pedir autorización a este; por lo que la Universidad debe estar preparada para pedir la autorización de toda persona que se vea involucrada en el proceso y sean requeridos sus datos.

Es de resaltar que la Universidad debe obtener esta autorización a más tardar al momento de recolectar los datos personales del titular de la información, según el artículo 5 del Decreto 1377 de 2013.

Es muy importante que si el tratamiento de los datos personales se realizó antes del veintisiete (27) de junio de 2013, el Responsable de los datos se comunique con los titulares de la información con el fin de refrendar las autorizaciones exigidas por la Ley y poder continuar con el tratamiento de sus datos.

No obstante si luego de intentar refrendar la autorización por parte de estos titulares, estos no solicitan la supresión de sus datos personales dentro de un término de treinta (30) días, la Universidad puede seguir haciendo uso de estos.

La Universidad puede prescindir de la autorización en los casos en los que la Ley se lo permita, por ejemplo ante urgencias médico-sanitarias, en virtud de su función pública, un mandato judicial o legal que releve el consentimiento, según lo permite la Ley 1581 de 2012 en su artículo 4°, literal c y específicamente en el artículo 10°.

Paso N° 11: Descripción de las bases de datos personales

Antes de desplegar los procesos de obtención de la información, es necesario que dentro de la Universidad se describa en detalle la base de datos que va a contener la información, indicando como mínimo:

- ✓ La Política de Tratamiento que se aplicará a la base de datos.
- ✓ La naturaleza de los datos que contendrá.
- ✓ El volumen y la cantidad de datos que se estima almacenar.
- ✓ El responsable de la base de datos y el encargado designado para administrarla.
- ✓ El tiempo hasta el cual esta base de datos va a ser usada.
- ✓ La manera cómo se van a recolectar los datos personales de los titulares.
- ✓ La naturaleza de los datos recabados indicando si existen datos sensibles.
- ✓ La especificación del área o dependencia que se encargará de manera directa del tratamiento.
- ✓ El contexto en el cual se recolectarán los datos que allí se contendrán.
- ✓ La existencia de algún requerimiento legal que establezca la necesidad de compartir la información con otra Universidad de la Administración Pública o con Universidades privadas o Públicas.

Si se tiene manejo de datos reservados, conforme a la descripción de la base de datos reservados, será necesario incluir además los siguientes elementos:

- ✓ Quienes (áreas o servidores públicos) podrán tener acceso a dichos datos.
- ✓ El procedimiento que certifique la idoneidad de la persona que vaya a tener acceso a esta información.
- ✓ Las formalidades y limitaciones a su acceso.
- ✓ Las personas a quienes definitivamente se les negará el acceso.
- ✓ Las medidas necesarias para proteger el material clasificado.

Se debe recordar que las bases de datos personales recopiladas por la Universidad, no pueden mezclarse en ningún momento con los datos propios de la Universidad, es decir que las bases de datos personales deben ser minuciosamente individualizadas y separadas de los demás datos administrados. La descripción de las bases de datos personales debe ser consignada en un rotulo que sea visible antes de consultar las bases de datos de manera interna.

En este aspecto la Universidad deberá estimar la manera más apropiada para incluir la descripción de los datos personales, la cual deberá incluirse a manera de portada antes de acceder a la información de las bases.

5 PUNTOS CLAVE