Editorial Derecho Civil Hoy
Spin-Off de la Universidad de Granada

Revista de Derecho Actual, Vol. IV (2017), ISSN: 2445-4001

Fecha de recepción: 23/09/2017 - Fecha de aceptación: 05/10//2017

RETOS DE LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE DATOS PERSONALES –SGDP- EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR EN COLOMBIA DESDE EL PRINCIPIO DE SEGURIDAD

SEBASTIAN ALFONSO RUEDA QUESADA[1]
Consultor Derecho y Nuevas Tecnologías

RESUMEN

El Estado Colombiano reglamentó el tratamiento de datos personales mediante la Ley Estatutaria 1581 de 2012. Esta norma define obligaciones en cabeza de organizaciones, que como las Instituciones de Educación Superior –IES- realizan continuamente procesos de administración de información personal de sus estudiantes, trabajadores, proveedores y miembros de la comunidad académica en general. El marco obligacional, incluye la adopción de medidas técnicas y administrativas soportadas en el principio de *seguridad*, por lo que la protección de datos además de tener un claro componente legal, hace sinergia con algunos aspectos de seguridad de la información. El trabajo propuesto aborda la construcción de un SISTEMA DE GESTIÓN DE DATOS PERSONALES al interior de las IES, resaltando un orden de actividades a seguir, amparado en las buenas prácticas de seguridad de la información, valoración de riesgos y la experiencia de consultoría jurídica y estratégica al interior de IES en Colombia que permiten acercarse desde el marco conceptual al escenario práctico.

ABSTRACT

The Colombian State regulated the processing of personal data through Law 1581 of 2012. This norm defines obligations in the head of organizations, which, like the Higher Education Institutions -IES-, continuously carry out processes for the administration of personal data of their students, workers, suppliers and members of the academic community in general. The mandatory framework includes the adoption of technical and administrative measures supported by the security principle, so that data protection, in addition to having a clear legal component, synergizes with some aspects of information security. The proposed work addresses the construction of a "SISTEMA DE GESTIÓN DE DATOS PERSONALES" within IES, highlighting an order of activities to be followed, based on good information security practices, risk assessment and legal consulting experience and strategic within the IES in Colombia that allow approaching from the conceptual framework to the practical scenario.

[1] Abogado de la Universidad Santo Tomás Bucaramanga. Se desempeña actualmente como consultor empresarial en temas de protección de datos, derecho y tecnología.

PALABRAS CLAVE

Datos Personales, Sistema de Gestión, Seguridad de la información, cumplimiento legal.

KEYWORDS

Personal Data, Gestion System, Information Security, Legal Compliance.

Sumario

I.- INTRODUCCIÓN. II.- APROXIMACIÓN A LOS CONCEPTOS DEL SISTEMA DE GESTIÓN DE DATOS PERSONALES –SGDP-. III.- EL PRINCIPIO DE SEGURIDAD DESDE LA SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LOS DATOS PERSONALES. IV.- RETOS EN LA IMPLEMENTACIÓN DEL SGDP. IV.I. Obtener un entendimiento del negocio. IV.II. Entender los objetivos de la IES. IV.III. Realizar valoración de los riesgos. IV.IV.- Desarrollar un plan estratégico continuo que integre puntos anteriores. V**.- CONCLUSIONES. REFERENCIAS BIBLIOGRÁFICAS**.

I.- INTRODUCCIÓN

El Estado Colombiano mediante la Ley Estatutaria 1581 de 2012 estableció el marco jurídico de la protección de datos personales. Dicha norma, tiene como objetivo principal:

> "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" [1]

La referida Ley, tiene como sujetos de protección a las personas naturales; mientras que los sujetos obligados se definen como los responsables y encargados del tratamiento (personas naturales o jurídicas que gestionan datos personales). Dentro de los sujetos obligados, se encuentran las Instituciones de Educación Superior –IES-, ya que para el desarrollo de sus procesos estratégicos, misionales y de apoyo requieren constantemente: recolectar, almacenar, usar, circular y suprimir información de sus estudiantes, trabajadores, proveedores, visitantes, entre otros sujetos, que hacen parte de la comunidad académica, haciéndoles acreedores de la calidad de **responsables del tratamiento[2].**

Al respecto, la Corte Constitucional en su calidad de máximo intérprete de la Constitución Política de Colombia a quien se atribuye el desarrollo constitucional de la protección de datos personales, ha referido en diversas ocasiones que los datos personales y su adecuado tratamiento es una práctica cercana al respeto del

[2] Literal e del artículo 3 de la Ley 1581 de 2012 define al responsable como: "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;"

principio de dignidad humana. Se concluye entonces que la protección de los datos personales al estar consignada en el artículo 15 fue reconocida por el Constituyente como un derecho necesario para la dignificación del hombre, en la medida en que su información personal no sólo revela su identidad sino que puede ser utilizada con fines no autorizados por su titular, en detrimento de sus derechos humanos y libertades públicas.

Por el panorama normativo expuesto, las IES deben implementar un SISTEMA DE GESTIÓN DE DATOS PERSONALES, que siga los lineamientos del principio de seguridad, encontrando un interesante referente en la norma NTC-ISO-IEC 27001-2013, lo cual responderá a la confianza de la comunidad académica que diariamente entrega información personal, optimizando sus procesos desde la cultura de gobierno de datos o de la información.[3][2]

II.- APROXIMACIÓN A LOS CONCEPTOS DEL SISTEMA DE GESTIÓN DE DATOS PERSONALES –SGDP-.

Un Sistema de Gestión de Datos Personales –SGDP- debe aterrizarse a los conceptos normativos y la realidad que viven las IES. Primero, es necesario interpretar que es un dato personal bajo la óptica de la Ley Colombiana. El literal c del artículo 3 de la ley 1581 de 2012 lo define como:

> *"Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;"*

Sin embargo, esta definición debe ser interpretada a la luz de los pronunciamientos jurisprudenciales, ya que la misma no es suficientemente clara frente al alcance del dato personal, pues la amplitud de su esencia permitiría afirmar que casi "toda" la información es un dato personal, tesis que no es cierta. Para aclarar, se acude a la Sentencia **C-748 de 2011**, (Magistrado Ponente: Jorge Ignacio Pretelt Chaljub), en la cual se expresó:

> *"En efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales - 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"*

Bajo esta precisión, se entiende por dato personal aquella información que refiere a una **persona natural**, identificándola o pudiéndola identificar por contener rasgos físicos, sociales, de ubicación, académicos, médicos o de su esfera personal. La propiedad del dato reside en la persona natural (entiéndase *titular*). El dato personal cuenta con diversos principios que rigen su tratamiento, pero puntualmente se hará énfasis en dos; principio de libertad y de seguridad.

[3] El concepto de gobierno de información o de datos se sintetiza así: "Es una disciplina encargada de la orquestación de gente, procesos y tecnología que permite habilitar a una compañía a apalancar la información como un recurso de valor empresarial, y al mismo tiempo, es la encargada de mantener a los usuarios, auditores y reguladores satisfechos, usando la mejora de la calidad de los datos para retener clientes, constituyendo y guiando a nuevas oportunidades en el mercado."

El principio de libertad es desarrollado en el artículo 4 de la ley 1581 de 2012 y establece que para realizar un tratamiento debe contarse con el consentimiento previo, expreso e informado del titular. En este orden, los datos no podrán ser divulgados u obtenidos sin previa autorización o en ausencia de mandato judicial legal o judicial que releve el consentimiento. La autorización en síntesis, es aquella manifestación de voluntad del titular –dueño de los datos- para que usen sus datos personales bajo las finalidades informadas, pudiéndose otorgar por tres (3) medios: "por escrito, de manera verbal, o por conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización" [5]. El principio de seguridad, por su amplitud, será desarrollado posteriormente.

La metodología definida para analizar las obligaciones legales que deben cumplir las IES, será a través de un proceso[4] que todas desarrollan y que permite aterrizarlo en la práctica. Hipotéticamente hablamos del proceso de "Gestión de Admisiones". [3] Este proceso tiene como objetivo:

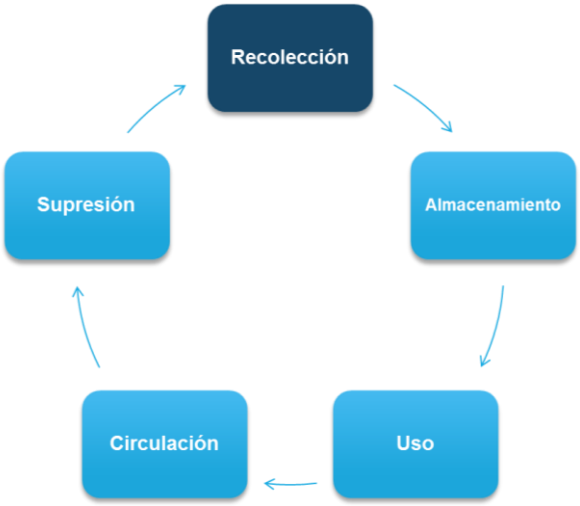
> "Seleccionar los estudiantes de primer ingreso en cada uno de los programas ofrecidos por la Institución de Educación Superior de manera eficiente, cumpliendo con los requisitos y reglamentación establecida"

Proceso que constituye una de las más grandes fuentes de recolección de información en cualquier IES, y es aquí en dónde la ley exige que el titular otorgue su autorización. La autorización generalmente, se sugiere incluir dentro del formato de vinculación, mediante la cual el aspirante acepta para que se utilizarán sus datos personales al interior de la IES y le informan de la existencia de la Política de Tratamiento de la Información de la Institución[5].

En este punto, hemos analizado la obligación legal desde la primera etapa del ciclo de vida del dato personal. En una IES la información personal es tratada bajo las siguientes actividades[6]:

[4] La norma ISO 9001 define a un proceso como: "Conjunto de actividades que están interrelacionadas y que pueden interactuar entre sí. Estas actividades transforman los elementos de entrada en resultados, para ello es esencial la asignación de recursos."
[5] La política de tratamiento de información es aquel documento maestro, en dónde se deben reflejar todos los aspectos fundamentales a tener en cuenta por la organización en el tratamiento de datos personales. En el mismo, se incluyen los principios y directrices que garantizarán la dignidad humana de los titulares de la información personal en razón a su tratamiento. El artículo 13 del Decreto 1377 establece sus elementos esenciales.
[6] La ley 1581 de 2012 define el tratamiento como "recolección, almacenamiento, uso, circulación y supresión de datos personales"

Fig. 1. Ilustración del ciclo de tratamiento del dato personal (recolección, almacenamiento, uso, circulación y supresión)



Pasando al almacenamiento, es donde aparece el principio de seguridad. El literal g, del artículo 4 de la ley 1581 de 2012 lo define como:

> *"La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, 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;"*

La corte constitucional mediante sentencia C-748 de 2011 dio alcance al principio de seguridad: [4]

> "En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos"
>
> Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria."

Y es aquí, donde el principio de seguridad al estar determinado por la ley 1581 de manera genérica sugiere remitirse a una norma técnica que aclare su alcance. En la revisión de constitucionalidad de la norma relacionada, ASOBANCARIA en calidad de tercero interviniente realizo las siguientes reflexiones sobre el principio seguridad y la forma en que se veía planteado en la Ley:

> "ASOBANCARIA afirma con respecto al literal g) del artículo 4 del Proyecto de Ley la expresión "que sean necesarias" genera dos interrogantes: ¿Quién determina que las medidas para asegurar la protección del dato, en un evento determinado, fueron las necesarias para garantizar la seguridad de los registros? y ¿Con base en qué criterios se puede determinar esto? La norma no ofrece respuesta a estos interrogantes. Esa ambigüedad en la regulación es la que permite advertir que una determinación abierta expone los Responsable a los criterios de una autoridad administrativa."

Situaciones que llevan a acércanos a la revisión del principio de seguridad en ámbitos no exclusivamente legales, sino técnicos y funcionales.

III.- EL PRINCIPIO DE SEGURIDAD DESDE LA SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LOS DATOS PERSONALES.

Sin lugar a duda, la protección de datos personales encuentra estrecha relación con la seguridad de la información[7]. Mientras, que la información constituye género, el dato personal lo hace en calidad de especie, por lo que, cualquier medida tendiente a proteger la información, puede ser útil cuando de cuidado y adecuado tratamiento de datos se refiere.

Uno de los referentes en seguridad de la información, es la norma técnica, NTC-ISO-IEC 27001-2013, [6] que tiene como objeto principal:

> "Brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple."

Se establecen objetivos y controles para determinar el nivel de implementación del SGSI. No obstante, no se centrará la atención en el SGSI, sino, el SGDP desde el principio de seguridad. Por ello, los insumos que otorga la ISO requieren que la IES cumpla una serie de pasos que permitan determinar qué medidas son necesarias para dar cumplimiento al principio de seguridad. Los mismos se reflejan así:

1. **Obtener un entendimiento del negocio:** Se debe realizar una identificación de la información que gestiona la IES, con qué finalidad y en dónde se almacena.
2. **Entender los objetivos de la IES:** Se deben comprender los objetivos estratégicos de la IES, para ver hacia dónde va, y que información requiere tratar para cumplir dicha planeación.

[7] La seguridad de la información es definida como: "Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad." [NTC-ISO/IEC 17799:2006]

3. **Realizar valoración de los riesgos:** Se deben aplicar metodologías de valoración de riesgos frente a la información identificada. Datos personales que, tengan naturaleza sensible, requieren mayores medidas de seguridad que otros tipos de datos.
4. **Aplicar controles que gestione riesgos:** Se debe establecer un plan que gestione los riesgos identificados. Algunos, de manera prioritaria atendiendo a la valoración de consecuencias e impacto.
5. **Desarrollar un plan estratégico continuo que integre puntos anteriores:** Se debe diseñar un Sistema de Gestión de Datos Personales a nivel de programa o plan estratégico. Las medidas de gestión de riesgo son iniciales, pero debe asignarse un responsable, procesos a cargo, instrumentos de medición, todo soportado en el apoyo de la alta dirección, que asegure continuidad al sistema.
6. **Disponer recursos necesarios para desarrollar el plan:** Se deben asignar recursos económicos, de talento humano y físicos para desarrollar el SGDP. La ISO hace una referencia valiosa: para requerimientos simples, sistemas simples y esta premisa debe permitir valorar que recursos se deben asignar.
7. **Supervisar, monitorear y actualizar los controles:** Todo Sistema debe ser en principio medible mediante supervisión de indicadores, metas y actividades. Posteriormente, debe mantenerse este seguimiento en pro de la mejora continua. Ningún sistema se diseña para no mejorar, y particularmente el de protección de datos personales es consiente que dar cumplimiento al 100% de las obligaciones legales no es tarea fácil. La pregunta no es si una IES cumple al cien por ciento (100%) la ley, sino: ¿Cómo cumplimos? ¿Cómo medimos? Y, ¿Cómo mejoramos continuamente?

IV.- RETOS EN LA IMPLEMENTACIÓN DEL SGDP.

Visto el plan de trabajo que plantea la Ley 1581 de 2012 desde el principio de seguridad, es necesario desarrollar los puntos que representan mayores retos al interior de una IES. Puntualmente, se analizarán los numerales **1, 2, 3, y 5.**

IV.I. Obtener un entendimiento del negocio

La IES debe identificar los macro procesos que desarrolla bajo los estándares de los Sistemas de Gestión de Calidad –SGC-. Macroprocesos estratégicos, misionales y de apoyo. Paso seguido, identificar los procesos que desarrolla en cada uno de los macro procesos. Siguiendo con el ejemplo, el proceso de Gestión de Admisiones es un macro proceso misional, pues desarrolla actividades directamente relacionadas al objeto social de la IES.

La pregunta que sigue es, en qué sedes desarrolla este proceso, ya que es común que las IES tengan diversos espacios físicos, algunos con procesos concentrados, para identificar posteriormente qué cargo al interior de la IES es responsable del proceso. En el ejemplo propuesto, podría decirse hipotéticamente que el responsable es el Director de Admisiones.

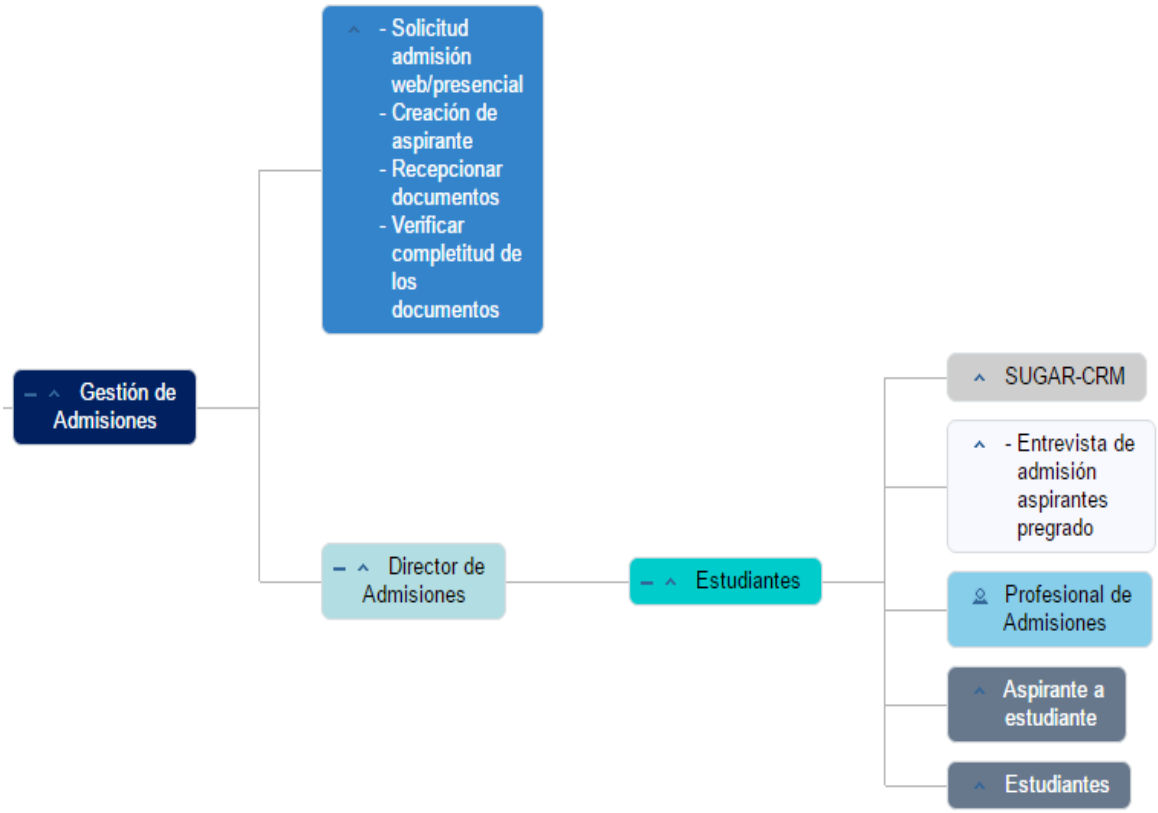
Una vez se ha entendido la estructura, viene el deber de identificar qué base de datos gestiona el proceso de gestión de admisiones. La ley 1581 de 2012 define a la base de datos en el literal b del artículo 3: “Conjunto organizado de datos personales que sea objeto de Tratamiento”. La base de datos puede ser de tratamiento automatizado o no automatizado. Esta base de datos solo puede ser utilizada para los fines, que quienes hacen

parte de ella han autorizado a la IES, y esto también debe identificarse y soportarse a través de la evidencia, respondiendo al principio de libertad.

Finalmente, se debe integrar el sistema de información que permite la consulta de la base de datos, que personas al interior de la IES acceden a ella, si pertenecen al mismo proceso de gestión de admisiones, u otro, y que terceros externos acceden en calidad de encargados del tratamiento[8].

El producto final de esta primera fase, es la consolidación de la estructura de gobierno de la información basada en protección de datos personales. A continuación, siguiendo con el ejemplo de gestión de admisiones se refleja una muestra:

Fig. 2. Ejemplo aplicado de la estructura de gobierno de información al proceso de gestión de admisiones.



[8] Literal d, artículo 3, ley 1581 de 2012 define al encargado del tratamiento como: "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;"

Revista de Derecho Actual, Vol. IV (2017), ISSN: 2445-4001

Fig. 3. Convenciones de interpretación del mapa de gobierno de información.

	Los cuadros de color azul oscuro representan el Proceso en que se realiza tratamiento de datos personales. El nombre del proceso se encuentra al interior del cuadro.
	Los cuadros de color azul celeste reflejan los responsables del proceso.
	Los cuadros de color azul brillante muestran el listado de subprocesos o procedimientos relacionados al proceso identificado de color azul oscuro los cuales realizan tratamiento de datos personales.
	Los cuadros de color azul aguamarina muestran las bases de datos asociadas al proceso.
	Los cuadros de color gris claro representan los sistemas de almacenamiento asociados a cada base de datos, los cuales pueden ser físicos o automatizados.
	Los cuadros de color blanco contienen la lista de formatos que soportan el tratamiento de información personal al interior de la IES, asociados a cada base de datos.
	Los cuadros de color gris oscuro simbolizan los Encargados del tratamiento o terceros externos a la organización que desarrollan una actividad de tratamiento sobre la información personal contenida en la base de datos a la que se encuentra vinculado. Este campo es opcional, atendiendo a la realidad de la **IES.**
	Los cuadros de color azul claro muestran la persona designada como al interior de la IES como Responsable de la base de datos.
	Los cuadros de color azul grisáceo muestran los tipos de titulares o personas naturales cuya información se encuentra almacenada en la base de datos a la que se asocia.

IV.II. Entender los objetivos de la IES

Una planeación estratégica requiere que todos los actores de la IES, especialmente quienes se vayan a involucrar en el proyecto, conozcan el deber legal que recae en la Institución de implementar ciertas medidas administrativas y técnicas que aseguren el debido cuidado de la información. Por esto, es necesario que la IES:

1. Identifique los actores principalmente involucrados (líderes de procesos que continuamente gestionen datos personales)
2. Identifique a los actores involucrados en plano secundario (personal administrativo que sin direccionar un proceso, está en constante tratamiento de datos)

3. Diseñe planes de capacitación, en la cual sensibilice y socialice la obligación legal, las bases de lo que será el SGDP, el deber de la IES de implementar una cultura organizacional basada en protección de datos, entre otras cosas.

IV.III. Realizar valoración de los riesgos

Antes de iniciar una valoración de riesgos, se deben identificar de manera general los controles sobre los cuales se aplicará el análisis de riesgos. Una metodología a proponer, es aplicar una matriz de línea base, amenazas, vulnerabilidades y riesgos a través de cada proceso identificado (por ello la importancia de hacer un verdadero mapeo de la información como el que se propone en el punto No 1).

Los controles sobre los cuales se evaluará cada proceso, se resumen en los Factores Legales de Conformidad[9] propuestos a continuación:

Primer Factor. Autorización: "Persigue la aquiescencia previa, expresa, explícita y consentida del titular de los datos personales, para la recolección y el posterior tratamiento de los datos personales".

Segundo Factor. Políticas de Tratamiento de la Información Personal: "Aquel documento maestro en donde se deben reflejar todos los aspectos fundamentales a tener en cuenta por la organización en el tratamiento de datos personales. En el mismo, se incluyen los principios y directrices que garantizarán la dignidad humana de los titulares de la información personal en razón a su tratamiento".

Tercer Factor. Deberes del responsable – encargado del tratamiento: "Imperativos de orden legal, que exigen a las EIES el cumplimiento taxativo de acciones tendientes a garantizar el debido cuidado de la información personal que está bajo su responsabilidad o cuidado".

Cuarto Factor. Ejercicio de los derechos de los titulares: "Son los mecanismos mínimos exigidos por la ley, para materializar el derecho de habeas data del titular del dato personal. Entiéndase: Acceso, Rectificación, Cancelación y Oposición (ARCO). Los mismos deben ser puestos a conocimiento al titular".

[9] El Factor Legal de Conformidad –FLC- se define como: Aquel presupuesto que enmarca diferentes disposiciones constitucionales, jurisprudenciales, legales, reglamentarias y de soft-law, que imponen obligaciones a cumplir por las IES que realizan tratamiento de datos personales".

Quinto Factor. Del Registro Nacional de Bases de Datos: "Exigencia legal que impone una serie de requisitos a la IES, encaminados a la caracterización de las bases de datos gestionadas por su cuenta y posterior inscripción ante la delegatura para la Protección de Datos Personales adscrita a la Superintendencia de Industria y Comercio –SIC- (autoridad que en Colombia realiza inspección, vigilancia y control sobre la materia) ".

Sexto Factor. Seguridad de la información: "Son las medidas apropiadas y efectivas desde el punto de vista técnico para la materialización de la Política de Tratamiento de la Información Personal en la IES. Las mismas fluctúan, atendiendo al tamaño y composición de la IES, así como de la naturaleza de la información que la misma gestiona y el componente tecnológico que apalanca esta operación".

El resultado de este ejercicio debe generar una matriz de riesgos que realice las valoraciones aplicadas al proceso de gestión de admisiones, como se presenta aquí:

Tabla 1. Matriz de riesgo aplicada al proceso de Gestión de Admisiones

Factores Legal de Conformidad[10]
Autorización
Proceso analizado
Gestión de Admisiones
Línea base
En el proceso de Gestión de admisiones la recolección de información personal de los aspirantes a estudiantes se realiza a través del formato de Entrevista de aspirantes a pregrado. Dicha documentación, no cuenta con las autorizaciones del tratamiento de datos exigidas por el Artículo 4 y 5 del Decreto 1377 de 2013.
Consecuencias
Los titulares de datos personales pueden aprovechar la ausencia de solicitud de autorización para pedir de manera formal a la Institución, que por medio de una consulta se indique en qué momento se otorgó la autorización, el carácter previo, expreso y explícito de la misma, exponiendo un claro incumplimiento legal efectuado por la Institución de Educación Superior
Impacto
3
Probabilidad
3

[10] Los cuadros señalados con color azul y texto en color blanco representan los criterios de evaluación o aplicación de la información del Proceso y el Factor Legal de Conformidad.

Nivel de Riesgo (Probabilidad x Impacto)
9
Tipo de Riesgo
Inadmisible
Políticas de Administración
Adecuación del procedimiento y formatos de Gestión de Admisiones, que incluye la correcta recolección de los datos personales
Responsable
Director de Admisiones
Seguimiento
Almacenar adecuadamente copia de la autorización que brinde el titular posibilitando su posterior consulta.

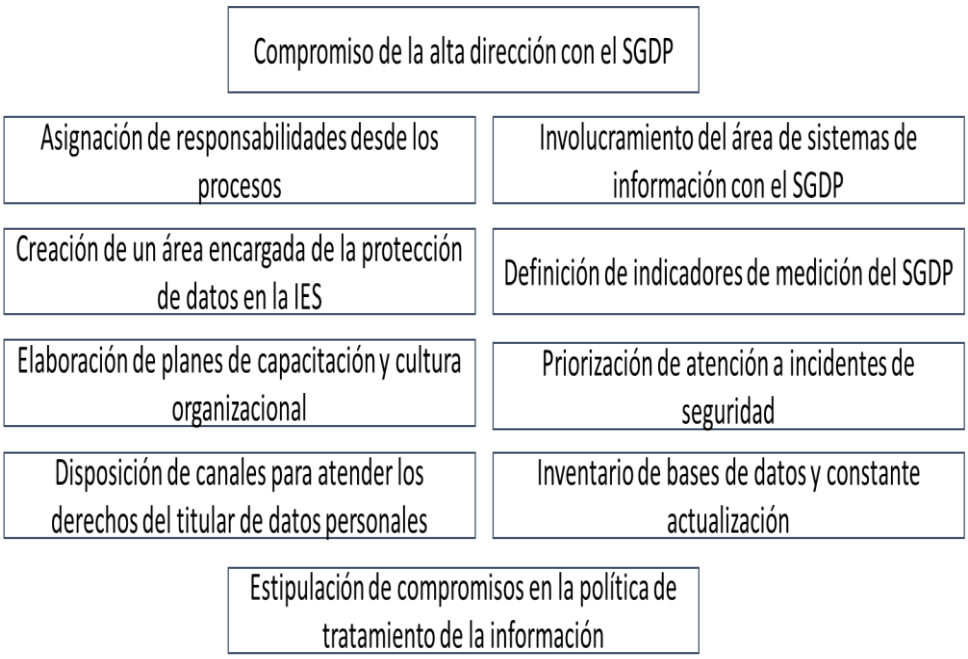
IV.IV.- Desarrollar un plan estratégico continuo que integre puntos anteriores

Con los insumos que se han venido recolectando, la IES ya está en capacidad de desarrollar un plan estratégico que persiga en primer momento mitigar los riesgos identificados (priorizando desde las consecuencias los que impacten en mayor medida la gestión de la información).

El plan estratégico debe reflejar algunos aspectos de lo que será la construcción del SISTEMA DE GESTIÓN DE DATOS PERSONALES en la Institución de Educación Superior –IES-.

Los puntos que debe contemplar el Sistema de Gestión de Datos Personales –SGDP- se relacionan a continuación:

Fig. 4. Cuadro de control de la implementación estratégica del SGDP.



El plan debe establecer claramente en cuanto tiempo se debe ejecutar (una IES requiere más de cuatro (4) meses por la complejidad de sus operaciones para desarrollar el plan), los recursos mínimos que requiere para ejecutar y la continuidad en el monitoreo y supervisión.

V.- CONCLUSIONES

La ley 1581 de 2012 estableció una obligación legal de cuidar la información personal en las IES. No obstante, el cómo hacerlo es otorgado por normas y metodologías técnicas, que como la NTC-ISO-IEC 27001-2013 establece un plan integral de implementación, que encuentra aspectos homologables a la ley 1581 de 2012, por la estrecha relación entre información y dato personal. En este sentido, la inclusión del principio de seguridad como uno de los guías en la interpretación de la ley 1581 de 2012, se da enhorabuena, pues, constituye un punto de partida inicial en como tomar medidas que realmente reflejen una correcta gestión de datos personales.

El presente artículo abordo la gestión de admisiones, siendo uno de los posibles elementos que invitan a comprender que la correcta gestión de datos personales, puede traducir mejoras a procesos internos de administración de información personal.

Pero, además de la gestión de admisiones, otros procesos al interior de las IES requieren intervención bajo la metodología propuesta, como lo son:

1. Manejo del expediente académico
2. Ayudas financieras/becas
3. Gestión de datos de los egresados
4. Actividades de comercialización con datos de menores de edad
5. Sistemas de copias de respaldo que aseguren la disponibilidad de los datos

6. Posibilidad de actualización periódica de los datos de los estudiantes
7. Interconexión de base de datos y sistemas de información
8. Atención oportuna de las consultas y reclamos generadas por los titulares de la información

Puntos que de cualquier manera requieren que previamente la IES haya realizado una identificación de gobierno de la información, pues cuando se habla de sistemas de gestión de datos personales y de seguridad de la información, se debe acudir al conocido mensaje que dice "antes de tomar la decisión de comprar un candado para la bicicleta, se debe estar seguro de que cuesta la bicicleta, pues se puede comprar un candado de dos millones para una bicicleta de un millón".

Todos los anteriores esfuerzos, respondiendo al respeto de la dignidad humana y derecho fundamental de la protección de datos personales, pues la revolución tecnológica que afrontamos ha enviado al ostracismo el regalo más grande que dejo la declaración universal de los derechos humanos suscrita en París (1948) y es situar al hombre, como centro de regulación y protección.

REFERENCIAS BIBLIOGRÁFICAS

1. Consulta de la norma Ley 1581 de 2012,
2. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
3. Software Specialty Architect, IBM México: https://www.ibm.com/developerworks/ssa/data/library/techarticle/gobierno-datos/)
4. Norma ISO 9001, http://www.nueva-iso-9001-2015.com/2014/11/iso-9001-entendiendo-enfoque-basado-procesos/
5. Sentencia C-748 de 2011, http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm
6. Consulta de la norma Decreto 1377 de 2013, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646
7. Norma NTC-ISO-IEC 27001-2013 http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf