El Reto de los Profesionales de Seguridad de la Información frente a la búsqueda de la Protección de Datos Personales en Colombia

Torres, Angela.
angela.torres1031@gmail.com
Universidad Piloto de Colombia

Resumen—La Ley Estatutaria 1581 fue publicada el 17 de Octubre de 2012, mediante esta ley se dictan las disposiciones para el tratamiento de los datos personales en Colombia; no obstante el 27 de Junio de 2013 se publicó el Decreto 1377 de 2013 el cual reglamento parcialmente la Ley 1581 de 2012. El pasado 13 de Mayo de 2014 se publicó el Decreto 886 de 2014, mediante el cual se reglamenta el artículo 25 de la ley 1581 de 2012, el cual se refiere al Registro Nacional de Bases de Datos. La publicación de esta ley y estos decretos mencionados anteriormente, muestra una evidente preocupación de la forma cómo en Colombia se venían vulnerando los derechos de los ciudadanos frente al tratamiento sus datos personales sin que se efectuara un control o se aplicará algún tipo de sanción a quienes realizaban dichos abusos. La publicación de la ley estatutaria 1266 del 31 de Diciembre de 2008, más conocida cómo Hábeas Data, se convirtió en el primer eslabón hacia la búsqueda de la protección de los datos personales en Colombia. Este documento pretende realizar un análisis de esta normatividad vigente y cómo su conocimiento y aplicabilidad sugiere un reto para los profesionales que nos dedicamos a la Seguridad de la Información.

Abstract— The statutory law 1581 was posted on October 17, 2012, by this law the provisions for the treatment of personal data in Colombia are issued; however the June 27, 2013 was published Decree 1377 of 2013 which partially Act 1581 Regulations 2012.

On May 13, 2014 was published Decree 886 of 2014, by which article 25 of Law 1581 of 2012, which refers to the National Registration Database is regulated.

The publication of this law and these decrees mentioned above, shows an evident concern the way in Colombia were being infringed the rights of citizens against their personal data treatment without a control is effected or some type of sanction applied to performed such abuses.

The publication of statutory law 1266 of December 31, 2008, better known as Hábeas Data, became the first step toward seeking the protection of personal data in Colombia.

This document aims to make an analysis of the current regulations and how their knowledge and applicability suggests a challenge for professionals dedicated to the Information Security.

Índice de Términos— Datos Personales, Encargado de los datos, Hábeas Data, Responsable de los Datos, Titular de los Datos.

I. INTRODUCCIÓN

Después de publicada el pasado 17 de Octubre de 2012 la Ley de Protección de Datos Personales más de un colombiano nos planteamos las siguientes preguntas, ¿Quién más tiene acceso a mis datos personales? ¿No se supone que son personales? El pasado 27 de Junio de 2013 se reglamento parcialmente la ley 1581 de 2012 a través del decreto 1377, por lo que la respuesta a la primera pregunta planteada tendría una respuesta.

Desde el mes de agosto de 2013, considero que para muchos de los colombianos fue una gran sorpresa recibir correos electrónicos de diferentes empresas solicitándonos la aprobación para el uso de nuestros datos personales; además de la sorpresa de haber recibido esos correos que antes de esa fecha no nos habían sido enviados con el mismo asunto y contenido, nos preguntamos ¿Porqué estas empresas tienen mis datos personales?, ¿En qué momento tuvimos algún contacto con ellos para que hubieran al menos registrado nuestros correos electrónicos en sus bases de datos?, ¿ Quién les facilitó esta información?

Fig. 1 ABC para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013. Tomado de http://colombiadigital.net/media/k2/items/cache/954882f62243d5d5e14df60ee84c324b_XL.jpg

En mi caso particular recibí correos electrónicos de empresas con las cuales no había tenido contacto, por ejemplo, recuerdo un correo que recibí con el asunto *Acuerdo para el registro de Información Personal*, de una revista llamada Practimotor perteneciente al grupo Practi S.A.S; estoy segura que nunca me inscribí en su página o facilité mi información para que este grupo la almacenara y menos la manipulara; de hecho ha sido el primer correo electrónico que recibí de parte de ellos; casos cómo estos escuche de diferentes personas y amigos después de la reglamentación de la Ley 1581 de 2012.

Es bastante preocupante darse cuenta que nuestra información personal ya no es tan personal y que se encuentra circulando por diferentes empresas cómo si les perteneciera.

"En Colombia se volvió una constante recibir llamadas telefónicas en las que se ofrecen toda clase de productos y servicios, desde seguros, cursos de inglés, tarjetas de crédito, electrodomésticos y viajes, entre otros. Nadie se escapa de esta práctica comercial que vienen usando las empresas y que tiene fastidiados a millones de colombianos que no saben cómo hacen las compañías para conseguir sus datos personales"[1].

La reglamentación de la ley 1581 es un paso adelante en Colombia para proteger la privacidad de nuestra información, pero también es claro que debería haberse reglamentado hace muchos años cómo en diferentes países del mundo en los cuales estás leyes se encuentran vigentes y haciéndose cumplir.

II. ¿QUÉ DICE LA LEY 1581 DE 2012 DE PROTECCIÓN DE DATOS PERSONALES?

Para dar respuesta a esta pregunta citaré el artículo 1 de la presente ley que dice: *"ARTÍCULO 1. 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"[2]*.

Esta ley se convierte entonces en una salvaguarda para toda la información que a través del tiempo las diferentes empresas y entidades han ido recolectando de cada uno de nosotros y de la cual hasta el momento no se tenía ningún control.

La ley 1581 impone la obligación a las empresas que tengan en sus bases de datos o en su poder datos personales y/o datos sensibles que hayan recopilado y almacenado antes de publicado el decreto 1377 de 2013, a solicitar autorización a los titulares de los datos para poder seguir almacenándolos y haciendo uso de ellos; es por esta razón que más de un colombiano recibimos tantos correos electrónicos solicitando dicha autorización; ya que las empresas pueden hacer uso de canales cómo llamadas telefónicas, cartas enviadas por correo certificado, avisos publicados en medios masivos de comunicación, correos electrónicos, entre otros, para solicitar dicha autorización.

Teniendo en cuenta lo anterior surge la pregunta, ¿Qué se considera cómo datos personales y datos sensibles?. La respuesta misma nos la da la ley 1581 de 2012; *"Para los propósitos de la presente ley, 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" [3].

La Figura 2 llamada Mapa Mental Ley 1581 de 2012, nos da una explicación de manera gráfica del la aplicabilidad de la misma y su interrelaciones.

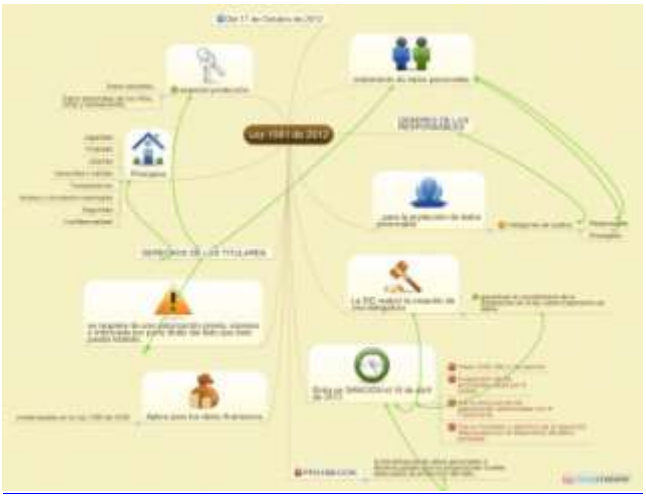

Fig. 2 Mapa Mental Ley 1581 de 2012. Tomado de http://jogacrack.co/20130408/mapa-mental-ley-1581-2012/

La ley 1581 de 2012 esta basada sobre 8 principios: Legalidad, Finalidad, Libertad, Veracidad o Calidad, Transparencia, Acceso y Circulación Restringida, Seguridad y Confidencialidad. Se identifican tres tipos de sujetos a saber, *el Titular de los Datos, el Responsable de los Datos y el encargado de los datos.* El titular de los datos es el dueño de los datos, es la misma persona en si de la cual sus datos pueden ser tratados, razón por la cual es requerida su autorización, expresa e informada para realizar dicho tratamiento.

El responsable de los datos es quién o quiénes toman decisiones sobre el tratamiento de los datos; este rol es bastante importante y delicado por esta razón la ley define explícitamente unos deberes a los responsables de los datos.

El encargado de los datos es quién o quiénes realizan el tratamiento de los datos. Cabe anotar que este dos roles pueden ser tanto personas naturales cómo personas jurídicas.

La ley 1581 de 2012 hace referencia a la protección especial de los datos personales y datos sensibles de los niños, niñas y adolecentes. La autoridad de protección de datos personales en Colombia definida en la ley 1581 es la Superintendencia de Industria y Comercio, la cual se encarga de garantizar el cumplimiento de lo que establece la ley. Realizado su trabajo cómo ente regulador la Superintendencia de Industria y Comercio en caso de incumplimiento deberá impartir sanciones hasta por 2000 SMLV. Además de la sanción económica la norma también define suspensión de actividades a las entidades hasta por seis meses, dictar el cierre temporal o definitivo de las operaciones relacionadas de tratamiento de datos sensibles en las entidades.

La ley 1581 de 2012 también establece que la transferencia de datos personales a otros países esta prohibida, si estos no tienen o no garantizan niveles apropiados de seguridad para la protección de dichos datos.

III. ¿QUÉ ES EL REGISTRO NACIONAL DE BASES DE DATOS?

La ley 1581 de 2012 en su artículo 25 mencionaba la creación de un Registro Nacional de Bases de Datos el cual fue reglamentado mediante el Decreto 886 del 13 de Mayo de 2014.

¿En qué consiste este macro proyecto?, ¿Cuál es su finalidad?. El Decreto 886 de 2014 nos da una idea de esta gran iniciativa del gobierno Nacional frente a la búsqueda de la protección de los datos personales de los ciudadanos colombianos.

"El registro nacional de Bases de Datos debe permitir a cualquier persona determinar quién está haciendo tratamiento de sus datos personales para de esa forma garantizar que la persona pueda tener un control efectivo sobre sus datos personales al poder conocer clara y certeramente en qué bases se manejan sus datos personales. Por ende, el Gobierno Nacional tendrá en su labor de reglamentación que acudir a los estándares internacionales y a la experiencia de otros Estados en la materia para lograr que la finalidad antes descrita de este registro se cumpla"[4].

Este macro proyecto busca que todas las bases de datos que estén bajo la regulación de la Ley 1581 de 2012 sean inscritas en el Registro Nacional de Bases de Datos. Este registro lo debe realizar el Responsable de los datos, sin importar si es de naturaleza pública o privada, persona natural o jurídica.

Dentro lo especificado en el Decreto 886 de 2014 existen algunos requisitos de información mínima que debe contener el Registro Nacional de Bases de Datos, los cuales son: Datos de identificación, ubicación y contacto del Responsable del Tratamiento de la base de datos; Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos; Canales para que los titulares ejerzan sus derechos; Nombre y finalidad de la base de datos; Forma de Tratamiento de la base de datos (manual y/o automatizada), y Política de Tratamiento de la información.

En este momento aún no se encuentra disponible el Registro Nacional de Bases de Datos y no fue establecido un plazo para que la Superintendencia de Industria y Comercio lo implemente, ya que por parte de la entidad obviamente es requerido contar con una infraestructura necesaria y suficiente para soportar este macro proyecto.

Cuando ya se cuente con la infraestructura disponible, la Superintendencia de Industria y Comercio informará de manera oportuna a los ciudadanos, ya que los Responsables de los datos tendrán un plazo establecido para realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de datos, el cual es de dos meses.

IV. ¿QUÉ DICE LA LEY 1266 DE 2008 ACERCA DE LA PROTECCIÓN DE DATOS PERSONALES?

Dentro del ámbito legislativo la primera ley que se acerco a esta iniciativa del gobierno Colombiano de proteger los datos personales de los ciudadanos es la Ley 1266 del 31 de Diciembre de 2008, conocida cómo ley de Hábeas Data.

Por medio de esta ley se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de países terceros, además de otras disposiciones.

De igual forma cómo en la ley 1581 de 2012, en la ley de Hábeas Data, se realizan algunas definiciones cómo por ejemplo, el titular de la información que puede ser una persona natural o jurídica a quien se refieren los datos personales, otra definición importante es la de fuente de información, que hace referencia a la organización u entidad que recibe o conoce los datos, cómo por ejemplo, un operador de telefonía móvil con el que un usuario ha celebrado un contrato.

Se denomina también a un operador de bancos de información quien recibe los datos personales de los titulares, los administra y los pone en conocimiento de los usuarios bajo los parámetros de ley, cómo por ejemplo, Datacrédito y CIFIN.

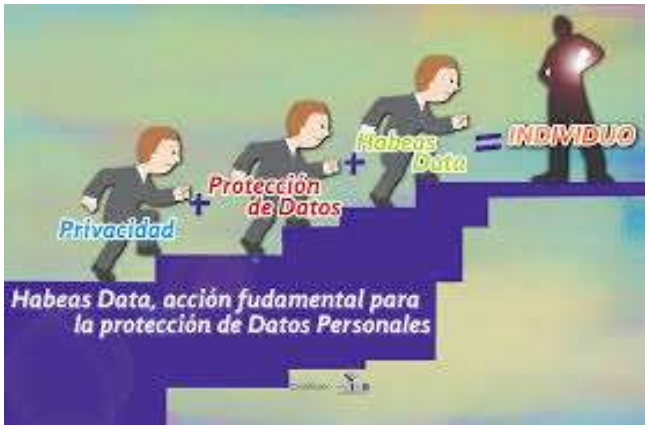

Fig. 3 Habeas Data, acción fundamental para la protección de datos personales. Tomado de http://www.imipe.org.mx/blog/2013/08/habeas-data/

"¿La actual regulación sobre hábeas data se refiere a toda la administración de los datos personales? No. La regulación actual sobre hábeas data, Ley 1266 de 2008, constituye una regulación parcial de este derecho, concentrada en las reglas para la administración de datos personales de carácter financiero, comercial, de servicios y proveniente de terceros países, destinada al cálculo del riesgo crediticio" [5].

V. ¿QUÉ DEBO HACER PARA RECLAMAR SOBRE EL DERECHO DE MIS DATOS PERSONALES?

Es importante tener claro que hacer si quiero que mi información personal sea eliminada, modificada o actualizada de las bases de datos donde se encuentra almacenada; de acuerdo a lo indicado en la ley 1581 de 2012, el artículo 15 menciona que se debe hacer llegar al responsable del tratamiento de los datos una solicitud donde se exprese claramente mi decisión, es importante que en esta solicitud se incluya la identificación del

titular, la descripción clara de los hechos que dan origen al reclamo, la dirección y se requiere adjuntar los documentos que sean necesarios para este trámite. En caso que la solicitud no se encuentre completa, hay 5 días hábiles para realizar las correcciones necesarias; cuando el reclamo se encuentra completo, la empresa debe indicar en sus bases de datos que existe un *reclamo en trámite* sobre esa información, esa leyenda debe permanecer hasta tanto se dé una respuesta sobre el reclamo realizado para el cual la empresa tiene 15 días hábiles para dar respuesta.

En caso de que no se reciba ninguna respuesta del reclamo radicado por parte de la empresa, el reclamo puede interponerse ante la SIC Superintendencia de Industria y Comercio, el artículo 19 de Ley 1581 dice:

"Artículo 19. Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley" [6].

VI. ¿CUÁL ES LA IMPORTANCIA DE MIS DATOS PERSONALES?

Esta pregunta es muy importante que cada uno de nosotros la interioricemos y ayudemos a formar conciencia de la importancia que tienen nuestros datos personales; un dato personal en malas manos puede estar siendo vendido en este momento en el mercado negro; incluyendo hasta nuestra huella digital, nuestro estado de salud, las enfermedades que padecemos, sin siquiera haber tenido acceso a nuestro historial médico. Los fines para los cuales puede ser usada nuestra información personal pueden ir hasta el punto de cometer delitos, ya que nuestra identidad puede ser suplantada en un momento dado.

Es una cruel realidad que hoy en día ninguna empresa, organización e individuo es inmune al robo de su información confidencial y datos personales, y menos a que estos sean comercializados en el creciente mercado negro de datos personales. Con el fin de evitar la suplantación de nuestros datos personales un aspecto clave es que conozcamos claramente a que tenemos derecho y cómo nos ampara la ley.

La revista dinero en una de sus publicaciones, hace claridad sobre algunos de los derechos que se estipularon a través del decreto 1377 de 2013, decreto que reglamentó parcialmente la ley de Protección de Datos Personales, los cuales se resumen en 7 ítems así:

Fig. 4 Protección de Datos Personales: Que no hay que hacer. Tomado de http://blogs.peru21.pe/atajosweb/protection-datos-personales-peru.jpg

"1. Los titulares de la información tienen derecho a encontrar de manera ágil y sencilla la información suministrada por ellos y que se encuentra bajo la administración de otros.

2. Los ciudadanos podrán consultar de manera gratuita sus datos personales, al menos una vez al mes, y cada vez que se generen cambios en las políticas de tratamiento de éstos.

3. En caso de no recordar haberse inscrito en una base de datos, el dueño de la información podrá solicitar una prueba de la autorización inicial por la que fue inscrito.

4. El propietario de los datos tiene derecho a que se le describa para qué y cómo será utilizada su información.

5. También se tendrá derecho a la actualización, rectificación y supresión cuando el titular lo considere conveniente (en cualquier momento) con sus propósitos o cuando el responsable por dicha información haya podido advertirlo para satisfacer los propósitos del tratamiento.

6. Todo administrador de la información deberá designar una persona o área que asuma la función de protección de datos personales, la cual también debe dar trámite a las solicitudes de los ciudadanos.

7. En caso de sentir que alguno de éstos derechos no son atendidos o cumplidos, el dueño de la información podrá recurrir al ente de control para radicar una queja formalmente" [7].

Conociendo que tenemos unos derechos sobre nuestros datos personales, *lo que no debemos hacer* es permitir que sin nuestra autorización estén en manos de entidades, organizaciones y personas inescrupulosas que puedan usarlas para actos delictivos, siempre que tengamos dudas sobre por que recibimos información de cierta entidad con la cual no tenemos ningún vínculo, o con la cual ni siquiera hemos establecido algún contacto, debemos solicitarles nos muestren evidencia de la autorización que hayamos dado para el tratamiento de nuestros datos.

Hagamos valer nuestros derechos cómo ciudadanos, démosle el valor que tienen nuestros datos personales y no permitamos más abusos.

VII. ¿CUÁL ES EL RETO DE LOS PROFESIONALES DE SEGURIDAD DE LA INFORMACIÓN FRENTE A LA PROTECCIÓN DE DATOS PERSONALES?

El análisis previo realizado sobre las leyes vigentes sobre Protección de Datos Personales, muestra que hay una gran responsabilidad individual y colectiva sobre este tema. Las organizaciones deben tener al interior, personal plenamente capacitado en seguridad de la información y seguridad informática para poder lograr este gran objetivo.

Desde el rol que desempeñemos dentro de las organizaciones, cómo profesionales dedicados a la seguridad de la información y seguridad informática, el reto es bastante grande.

Ahora veremos algunas de las más importantes estrategias, acciones y mejoras que cómo especialistas en esta área debemos procurar hagan parte de las metas que haya que alcanzar para el cumplimiento de este gran reto de protección de datos personales.

El conocimiento en material legal específicamente en protección de datos personales es la primera meta que cómo profesionales de seguridad de la información debemos tener.

Recuerdo que uno de los docentes de la especialización hizo hincapié en que un excelente oficial de seguridad o gerente de seguridad de la información, era aquel que no solamente contaba con el conocimiento técnico de ataques, software malicioso, vulnerabilidades o que era un experto hacker, sino aquel que también contaba con el conocimiento de seguridad de la información y su correcta gestión enfocándolo al logro de los objetivos de negocio de la compañía y el cumplimiento regulatorio.

Fig.5 Responsable de Seguridad. Tomado de http://www.om.df.gob.mx/media/dpersonales/capidapes/c06112012g.png

El énfasis en el conocimiento de las leyes colombianas aplicadas a la Seguridad de la información, los delitos informáticos, la seguridad de los datos personales y los derechos, es algo fundamental en lo que debemos esforzarnos por capacitarnos cada día más para poder contar con una alta competencia en este campo. Teniendo en cuenta esta necesidad, es muy importante que los profesionales dedicados a la seguridad de la información también conozcan de la ley y el derecho, para que al conjugar este conocimiento estemos en la competencia de formular, diseñar, implementar, evaluar y mejorar planes estratégicos de seguridad de la información que garanticen un nivel alto en las organizaciones en cuanto a la protección de los datos personales y protección de la información.

Cómo Responsables de la Seguridad de la Información dentro de las organizaciones, nuestra más importante labor es proteger la información personal haciendo uso de las medidas necesarias y pertinentes para evitar riesgos tales cómo el uso, modificación, destrucción, pérdida y revelación indebida.

Hay que tener en cuenta que las medidas que se implementen dependen del grado de sensibilidad de la información de la cual se esté realizando tratamiento o de la cual se esté cómo responsables de los datos. Las siguientes son algunas estrategias que cómo responsables de seguridad debemos velar por que se implementen.

Planes de Auditoría en Protección de Datos Personales: Cómo responsables de seguridad de la información dentro de las organizaciones, uno de los planes infaltables que debemos promover son la realización de auditorías de protección de datos personales de manera regular, estas auditorías podrían ser internas o externas; con el fin de evaluar el estado actual y mejora continua de este proceso dentro de las organizaciones. De esta manera se lograría verificar acciones correctivas y acciones de mejora encaminadas a cumplir con lo establecido en las leyes Colombianas, lo cual es supervisado a través entes regulatorios y autoridades. En una entidad u organización que haga las veces de Responsable de los Datos, estas auditorías deberán llevarse a cabo incluyendo las instalaciones de procesamiento de datos y las actividades de procesamiento.

Los resultados obtenidos de dichas auditorías deberán comunicarse a la junta directiva o alta dirección de la compañía, pero también es necesario que estén a disposición de los Responsables directos del tratamiento de los datos dentro de las organizaciones. Es muy probable que la autoridad de datos personales en nuestro país (Superintendencia de Industria y Comercio) dentro del proceso de mejora continúa de la aplicación de las leyes de protección de datos personales, solicite más adelante los resultados de dichas auditorías para realizar seguimiento sobre las actividades que se han venido realizando para garantizar la seguridad y protección de los datos personales cómo responsables de los datos.

Consultoría frente a la Protección de Datos Personales: Una consultoría con personal altamente calificado en protección de datos personales, es una excelente alternativa para identificar las falencias de las organizaciones frente al tema y los cambios deseados de cara al cumplimiento de las leyes vigentes en cuanto a protección de datos personales. La Consultoría debería incluir varias fases; para comenzar se debe realizar una revisión y levantamiento de información que determine que datos personales están bajo la responsabilidad de la organización, cual es el tratamiento que se les ha dado, se encuentra autorizado su uso y manipulación por parte del titular, entre otras. Luego de tener un marco de referencia sobre el tratamiento de los datos y el alcance del mismo dentro de la organización, se debería realizar un análisis técnico, jurídico y archivístico con el fin de verificar dentro de estos tres ítems, los procedimientos internos con los cuales se esta realizando el tratamiento de los datos y determinar cuales son las falencias en dichos procedimientos, definir unas metas y mejoras para los mismos; esto con el fin de dar cumplimiento a la legislación en Datos Personales y las obligaciones para la compañía en materia de hábeas Data.

A este análisis previo, se debe adicionar un análisis de Riesgos, en el cual a través de una matriz de riesgos se especifiquen los riesgos de tipo administrativo, penal, reputacional y económico. Este análisis de riesgos es determinante para identificar las posibles vulnerabilidades y amenazas que se encuentren presentes frente al tratamiento de los datos personales dentro de la organización y sus causas. Conocedores de esto se pueden prever y cuantificar a nivel económico los posibles daños y consecuencias que se pueden producir. Habiendo identificado las amenazas a las que se enfrenta la organización en cuanto al tratamiento de datos personales, la consultoría planteará una serie de recomendaciones a nivel de seguridad informática que estarán enfocadas en el fortalecimiento de la seguridad en los sistemas de información, los equipos de comunicaciones, equipos de seguridad perimetral, bases de datos, almacenamientos, servidores, redes de datos a nivel LAN y WAN; y optimización y maximización en los casos que sean requeridos. Esta serie de recomendaciones se generarán luego de realizadas las pruebas de hacking ético y un estudio del procedimiento de HARDENING sobre la infraestructura de la organización.

Además de las recomendaciones a nivel técnico (Seguridad Informática), la consultoría deberá entregar recomendaciones en cuanto a protección de datos personales en materia jurídica, con el fin de asesorar el diseño, caracterización, implementación, evaluación, gestión y documentación de los procesos que sean requeridos dentro de la organización, alineados a las mejores prácticas y mejores marcos de trabajo del mercado; con el fin de garantizar el cumplimiento a las leyes de protección de datos personales y evitar investigaciones y sanciones por parte de los entes de control.

Planes de Capacitación Continuas y Permanentes en Protección de Datos Personales: Debe existir un programa de entrenamiento adecuado en las leyes colombianas para protección de datos personales para los empleados dentro de las compañías que procesan los datos, o que tienen la responsabilidad del tratamiento de los datos de manera directa. No hay que descartar el entrenamiento y capacitación a nivel general a las distintas áreas de la organización en protección de datos personales, el cual debe convertirse en un plan liderado por él o los responsables de seguridad de la información dentro de las organizaciones.

Dentro de esta estrategia de capacitaciones, se deben incluir temas relacionados con el tratamiento legítimo de datos personales a nivel internacional, ya que teniendo en cuenta el tipo de negocio al que se dedique una compañía u organización, el desconocimiento de las regulaciones y estándares a nivel internacional que ya se encuentran definidos y que también están en concordancia a la ley estatutaria 1581 de 2012, puede convertirse en un riesgo.

En el ámbito de protección de datos personales a nivel internacional es una necesidad explicar varios conceptos clave que deben conocer quienes realizan negocios a nivel internacional, en los cuales están implícitas bases de datos con información de tipo personal o datos personales.

A continuación realizaré algunos apuntes en cuanto a esto.

¿Qué son las normas corporativas vinculantes NCV? "Son esquemas auto-regulatorios de protección de datos desarrollados originalmente en Europa con el ánimo de facilitar las transferencias de datos internacionales; resultan ser un instrumento para facilitar las transferencias de datos internacionales hacia destinos que no cuentan con un nivel apropiado debido a la garantía que ofrece la empresa exportadora de datos sobre el nivel adecuado de tratamiento de los mismos por parte de la entidad importadora" [8].

Otro concepto importante a incluir en dentro los procesos de capacitación en protección de datos personales a nivel internacional, tiene que ver con los Principios GAPP (Principios de Privacidad Generalmente Aceptados), los cuales apoyan a las empresas a cumplir las normas de privacidad y fomentar el uso de las buenas prácticas empresariales en protección de datos.

Estos principios se convierten en herramientas para las compañías, las empresas certificadoras, empresas de auditoría y las autoridades de protección de datos; para garantizar la eficacia y efectividad que tienen las NCV para probar un nivel adecuado de protección de datos personales, con el ánimo de generar una cultura empresarial positiva.

Recordemos que el eslabón más débil en cuanto a seguridad de la información son las personas, es muy importante que la estrategia y el plan de capacitación en protección de datos personales se convierta en una meta bastante relevante y que se realice a todos los niveles de la organización.

Para finalizar cito una frase que encierra un nivel de profundidad de la importancia de la protección de datos a nivel empresarial.

Convertir "la protección de datos en un elemento integral de la forma como una compañía hace negocios"[9] es un gran reto al cual nos encontramos enfrentados como responsables de seguridad de la información independientemente del rol que desempeñemos en las distintas organizaciones.

VIII. CONCLUSIONES

En el ejercicio profesional de la seguridad de la información es una necesidad volvernos expertos en el campo legal y normativo, especialmente en un tema tan álgido, de gran importancia y relevancia cómo es la protección de los datos personales. El estudio de las leyes y decretos realizados en este documento y su relación con las responsabilidades y

retos que esto impone a los responsables de seguridad de la información en las organizaciones es un tema de gran interés; se buscó además de mostrar esta relación, proponer algunas estrategias que apoyen el logro de este reto dentro de las organizaciones no solo a nivel nacional sino también tocando una pequeña parte del ámbito internacional.

Un trabajo más a profundidad para extender este estudio, es llegar a un punto de detalle más específico del Registro Nacional de Bases de Datos cuando entre en funcionamiento y en cuanto a la protección de datos personales a nivel internacional; cómo estar preparados y capacitados para cumplir con estos estándares y las leyes internacionales vigentes en cuanto protección de datos y así poder asesorar a las organizaciones en la implementación de las mejores prácticas de procesos de protección de datos personales.

Elaborado por:
Ángela Y. Torres C.
Estudiante Especialización Seguridad Informática
Universidad Piloto de Colombia
2014

REFERENCIAS

[1] Sociedad Colombiana de Archivistas (2012, Agosto). La Información un Asunto Personal. Disponible: http://www.scarchivistas.org/la-informacion-un-asunto-personal/
[2] Ley Estatutaria 1581 (2012,Octubre) Objeto, Ámbito de Aplicación y Definiciones. Articulo1. Pág.1.
[3] Ley Estatutaria 1581 (2012,Octubre) Categorías Especiales de los Datos. Articulo 5. Pág. 4.
[4] Decreto 886 (2014, Mayo) Consideraciones. Pág. 1
[5] Superintendencia de Industria y Comercio. Manejo de Información Personal 'Hábeas Data'.Disponible: http://www.sic.gov.co/drupal/manejo-de-informacion-personal
[6] Ley Estatutaria 1581 (2012, Octubre) Autoridad de Protección de Datos. Articulo 19. Pág. 10
[6] Revista Dinero. Sus derechos en el Hábeas Data. Disponible:http://www.dinero.com/pais/articulo/sus-derechos-habeas-data/181020
[8] Superintendencia de Industria y Comercio. Estudio sobre la aplicación de normas corporativas vinculantes en el escenario internacional. Disponible: http://www.sic.gov.co/drupal/sites/default/files/files/Estudio_SIC_NCV.pdf Pág. 8
[9] Superintendencia de Industria y Comercio. Estudio sobre la aplicación de normas corporativas vinculantes en el escenario internacional. Disponible: http://www.sic.gov.co/drupal/sites/default/files/files/Estudio_SIC_NCV.pdf Pág. 12