LA PROTECCIÓN DE DATOS PERSONALES COMO SISTEMA DE GESTIÓN

Portilla Moya, César Augusto
capcompany@gmail.com, capcompany@hotmail.com
Universidad Piloto de Colombia

Abstract – The Compliance with legal regulations related to the protection of personal data in Colombia is mandatory for every public and private entity. This paper presents a protection scheme of personal data through the implementation of a Management System, that allows any organization of any kind have a framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the security of personal data in compliance with current legal regulations in Colombia.

Resumen – El cumplimiento de la normatividad legal relacionada con la protección de datos personales en Colombia es de carácter obligatorio para cualquier entidad pública y privada. Este artículo plantea un esquema de protección de datos personales a través de la implementación de un Sistema de Gestión que permita a cualquier organización de cualquier naturaleza, tener un marco de referencia para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de la seguridad de los datos personales en cumplimiento con la normatividad legal vigente en Colombia.

Índice de Términos— Sistema de Gestión de Seguridad de Datos personales, cumplimiento legal, datos personales, información, seguridad de la información.

I. INTRODUCCIÓN

La sociedad actual se considera como la sucesora de la sociedad industrial (sociedad capitalista), en algunos casos es denominada la sociedad de la Información y en otros como la sociedad del conocimiento; autores como Yoneji Masuda[1] la definen como: La "Sociedad que crece y se desarrolla alrededor de la información, aportando un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material". Por su parte Peter Drucker[2] la ha denominado la sociedad del conocimiento, definiéndola como el lugar donde la información que circula es la materia prima que es transformada en conocimiento, convirtiéndose éste, en el recurso con mayor grado de importancia por encima del trabajo, la tierra y el capital.

Sin importar cuál sea la mejor denominación atribuida a la sociedad actual por parte de los científicos sociales, la información y el conocimiento basado en la información, son el motor de creación omnipresente, sobre la cual se gestan innumerables modelos de negocio, se construyen imperios económicos y se transforman sociedades.

Como tal la información es definida como "un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje"[3]; esta puede ser sometida a múltiples clasificaciones dependiendo del contexto donde sea interpretada, sin embargo se podría analizar la información desde dos tipos de enfoque, uno asociado a la información empresarial y por otro asociado a la información personal (datos personales).

Desde el enfoque empresarial, la información ha llegado a catalogarse como el activo de mayor valor de cualquier organización, ya que es un recurso instrumental no finalista, un vehículo de generación de ideas, herramientas, metodologías, estrategias, servicios y productos; su aseguramiento y la preservación de los principios de -confidencialidad, integridad y disponibilidad-, es una prioridad con tal grado de compromiso que diferentes organismos internacionales, se han reunido para desarrollar estándares que incorporen las mejores prácticas con el fin de que las organizaciones de cualquier sector, implementen Sistemas de Gestión de Seguridad de la Información, que le permitan administrar de manera segura su información y los activos asociados a la misma.

Vista desde el enfoque de información personal (dato personal), se puede determinar que la información cobra importancia y valor de manera inherente ya que a través de ella podemos identificar, contactar y localizar personas, incluso puede llegar a asociarse con fuentes de masificación como las tecnologías de la comunicación y las redes sociales, para construir nuevos mecanismos de integración entre individuos y nuevas formas de identidad propia; su tratamiento y utilización también hacen parte de los modelos económicos de la sociedad actual, siendo una fuente rentable para las empresas que basan sus operaciones en la misma o se apoyan en ella para su ejecución, pero al mismo tiempo pueden ser parte del recurso utilizado por gobiernos,

[1] MASUDA, Yoneji. La sociedad informatizada como sociedad post-industrial. Madrid: Fundesco Tecnos, 1984

[2] Abogado de origen austriaco considerado como el mayor filosofo de la administración, reconocido como padre y mentor de la sociedad del conocimiento.

[3] http://es.wikipedia.org/wiki/Informaci%C3%B3n Consulta: lunes 01 de septiembre de 2014.

autoridades e incluso delincuentes para lograr la individualización de cualquier tipo de persona.

Como tal la información personal está conformada por los datos personales, estos están definidos como "cualquier información vinculada o que pueda asociarse a una o varias personas determinadas o determinable"[4], su protección puede estar amparada de manera indirecta por los estándares que permiten la implementación de los Sistemas de Gestión de Seguridad de la información; sin embargo por su nivel de criticidad e importancia dentro de la sociedad y con el fin de garantizar los derechos constitucionales contemplados en el artículo 15[5] de la constitución Política Nacional de Colombia, se han proclamado normativas específicas que buscan regular su tratamiento a través de leyes y decretos; entre ellos cabe señalar la ley 1266 de 2009, la ley 1581 de 2012, el decreto 1377 de 2013 y el decreto 886 de 2014.

Como tal cada normativa tiene por Objeto:

Ley 1266 de 2009 ―*…desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política,* ***particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países***"

Ley 1581 de 2012 "…. *desarrollar el derecho constitucional que tiene 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//.*

Decreto 1377 de 2013 "…*reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*."

Decreto 886 de 2014 "… *Reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento//.*

Tanto las leyes como los decretos referidos, buscan establecer los principios, deberes, derechos, garantías, procedimientos autoridades y sanciones referentes al tratamiento de los datos personales; sin embargo a pesar de los esfuerzos realizados por el gobierno nacional en materia legislativa, no se ha publicado hasta la fecha alguna guía que permita a las entidades públicas y privadas, tener un marco de referencia para realizar una apropiada implementación de la normatividad relacionada a la protección de datos personales, que sea acorde con las características de las organizaciones y que permita autoevaluar el estado del cumplimiento de la normatividad, más allá del alcance de una lista de chequeo de requerimientos.

Las cifras de quejas, reclamos e investigaciones van en aumento cada día, es por ello que es preciso contar con los modelos necesarios que nos permitan gestionar correctamente la protección de datos personales y adquirir una cultura de buenas prácticas frente a ello.

Fig. 2: Quejas de vulneración de datos personales año 2014. Fuente: Superintendencia de Industria y Comercio

¿Por qué no basar la implementación del cumplimiento de la normatividad de protección de datos personales con un modelo conocido y ya definido? Un modelo de gestión basado en el ciclo PHVA, planear, hacer, verificar y actuar; enfocado a la protección de datos personales puede funcionar como una herramienta hibrida que logre potenciar la gestión, la seguridad y el cumplimiento normativo.

II. SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

Se podría suponer desde un enfoque holístico, que mediante la implementación de un Sistema de Gestión de Seguridad de la Información, podría ser cubierto el cumplimiento de la normatividad de protección de datos personales, tan sólo basándose en el cumplimiento de los requerimientos y de los controles contemplados en estándares internacionales como los de la norma ISO 27001, sin embargo es necesario precisar que no todas

[4] Articulo 1 literal c, Ley estatutaria Nº 1581 de 2012

[5] "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…"

las organizaciones, están obligadas o están interesadas en realizar la implementación de estándares internacionales, ya sea porque no hace parte de las exigencias contractuales, no existe normatividad legal sectorial y obligatoria, o porque los stakeholders[6] no ven en la implementación un valor agregado o diferencial para su negocio.

La implementación de un Sistema de Gestión de Datos Personales es factible, toda vez que la normatividad en protección de datos personales es de obligatorio cumplimiento, aplicable a organizaciones públicas y privadas de cualquier tamaño, y de cualquier sector empresarial. Al basar la implementación de la normatividad de protección de datos personales en un modelo de gestión, se podrá desarrollar un marco que permita el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del cumplimiento legal. Se presenta a continuación una alternativa hibrida de un Sistema de Gestión de Seguridad de Datos Personales, desde una perspectiva general, basada en la experiencia del autor de este artículo[7] , el estándar ISO 27001, y en la guía para implementación de un Sistema de Gestión de Seguridad de Datos Personales propuesto por el **Instituto Federal de Acceso a la Información y Protección de Datos** (IFAI) de México.

III. ENFOQUE BASADO EN PROCESOS

Un Sistema de Gestión de Seguridad de Datos personales como todo sistema de gestión, debe basarse en procesos, la alta dirección de cualquier entidad debe identificar los procesos estratégicos, misionales y de apoyo, entender cuáles son los elementos de entrada, la forma en que se gestionan y cuáles son los resultados. Es importante identificar los procesos en que se hace tratamiento de datos personales, su flujo a través de los diferentes procesos de la organización, su ciclo de vida, el tratamiento que se hace sobre los mismos, los activos sobre los cuales se soporta su gestión y el análisis de riesgos de la información, entendiendo cuál de estos procesos sufriría mayor afectación, y generaría mayor impacto para la organización en el evento de materializarse un riesgo, de esta forma se podría establecer los procesos prioritarios para iniciar la implementación de la normatividad de protección de datos personales.

IV. CICLO PHVA EN EL SISTEMA DE GESTIÓN DE DATOS

El Sistema de Gestión de Seguridad de Datos Personales no solo permite el cumplimiento de la normatividad legal, sino incorpora buenas prácticas para la correcta gestión de la seguridad de los datos personales, un modelo basado en la norma ISO 27001, diferencia cuatro fases: Planear, hacer, verificar, actuar; cada una de las fases contiene una serie de actividades que a su vez se subdividen en tareas.

Fig. 2: Ciclo PHVA. Fuente: www.engestion.com

A. FASE: PLANEAR

Esta fase deberá comprender todo el diseño y planeación de las actividades o labores principales que soportarán la mayor parte del Sistema de Gestión, se deberá tener en cuenta las tareas o labores derivadas que se desprenden de cada actividad, los tiempos, y los recursos necesarios para llevar a cabo cada una de las labores principales y derivadas, entre ellas se consideran las siguientes:

1. Alcance y Objetivos: Actividad donde se realiza la contextualización de las áreas y los procesos donde se implementará el sistema de gestión de datos personales dependiendo de su criticidad, de igual manera se definirá el objeto por el cual se realiza la implementación del sistema de gestión de acuerdo a las expectativas de todas las partes interesadas.

2. Política de Protección de datos personales: El compromiso formal documentado de la Alta Gerencia hacia el tratamiento adecuado de datos personales en la organización.

3. Determinación de obligaciones y responsabilidades:

   3.1. Identificación de la normatividad sectorial aplicable.

   3.2 Determinación de las obligaciones y excepciones legales según el tipo de dato tratado (público y/o sensible) y según la calidad del tratante (responsable, encargado, usuario).

   3.3 Determinación de las responsabilidades contractuales.

4. Caracterización de la información personal:

   4.1 Definición de las actividades internas de cada proceso del área donde se hace el tratamiento de la información.

[6] El término agrupa a trabajadores, organizaciones sociales, accionistas y proveedores, entre muchos otros actores clave que se ven afectados por las decisiones de una empresa

[7] Portilla Moya César Augusto.

4.2 Identificación del flujo de información personal dentro de las actividades y procedimientos.

4.3 Identificación de los tipos de información personal.

4.4 Identificación de la finalidad del tratamiento de información personal.

4.5 Determinación del tratamiento realizado a la información personal (acceso, actualización, supresión, modificación, etc.)

4.6 Determinación de las Fuentes y mecanismos de obtención de información personal.

4.7 Ciclo de vida del dato personal.

4.8 Identificación de los terceros con quien se realiza el Intercambio de información personal.

4.9 Caracterización de los activos de información utilizados en el tratamiento de la información personal (bases de datos, repositorios físicos y digitales, sistemas de información, etc.).

4.10 Evaluación del riesgo de los datos personales: Identificación de amenazas, vulnerabilidades, riesgo, nivel de riesgo, probabilidad de la materialización de un riesgo impacto.

4.11 Identificación de las medidas necesarias para la mitigación del riesgo.

B. FASE: HACER

En esta fase se establecen y ejecutan:

1. Plan de operación del SGSDP.
2. Plan de recursos necesarios para operar el SGSDP.
3. Las políticas, procedimientos, guías, instructivos y formatos necesarios para el correcto tratamiento de la información personal.
4. Los planes de tratamiento de riesgos que garantizan la seguridad de la información personal.
5. Implementar la lista de controles[8] que permitirán dar cumplimiento a la norma.
6. Plan de Trabajo para la Implementación de las Medidas de Seguridad administrativas, técnicas, humanas y administrativas.
7. Programas de capacitación y entrenamiento para los terceros internos y externos con los que se intercambia información.
8. El plan de divulgación de las políticas de protección de datos personales y las recomendaciones de seguridad.
9. Asignación de los roles y responsabilidades de quienes hagan tratamiento de los datos personales en la organización y quienes vayan a ejecutar las tareas de la fase de planeación.
10. Programas de auditoría (Se propone y se ejecuta en la fase de verificar).

C. FASE VERIFICAR

En esta fase se debe evaluar el funcionamiento del SGSDP teniendo en cuenta el monitoreo, revisión y controles para:

1. Identificar los errores en los procedimientos diseñados para el tratamiento de la información personal.
2. Evaluar los resultados de la implementación de las políticas, planes, procesos y procedimientos.
3. Evaluar que las medidas tomadas para realizar el tratamiento de la información personal estén funcionando como se esperaba.
4. Detectar los eventos que pueden exponer a la organización al no cumplimiento de la normatividad.
5. Identificar los incidentes e inconsistencias que causan el incumplimiento de la normatividad.
6. Medir la efectividad de los procedimientos para verificar que se cumplan con las obligaciones normativas legales y contractuales.
7. Revisar las evaluaciones de los riesgos a intervalos definidos, teniendo en cuenta los niveles de riesgo, teniendo en cuenta:
   a) Modificaciones en el contexto de la organización
   b) Cambios en la tecnología asociada al tratamiento de la información personal.
   c) Variaciones de los objetivos y procesos comerciales.
   d) Aparición de nuevas amenazas.

[8] Se sugiere que al igual que la "Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales del IFAI ", para el cumplimiento de la normatividad mexicana, se proceda a generar para la normatividad colombiana una lista de requisitos desglosados a cumplir que funciones como controles

e) Efectividad de las medidas de seguridad implementadas.

f) Factores externos de cambio en la normatividad y acuerdos contractuales.

De igual manera se tiene que hacer un proceso de revisión mediante:

8. Auditorías internas a intervalos definidos para determinar el desempeño del SGSDP.

9. Registro de las acciones y eventos que podrían tener un impacto sobre la efectividad del SGSDP

D. FASE ACTUAR

La revisión de los resultados de las auditorías proporcionan información que permite demostrar la eficacia del SGSDP, de igual manera aporta la información necesaria para identificar las áreas de oportunidad donde éste puede ser mejorado, a través de:

1. La aplicación de acciones correctivas y preventivas.

2. Reevaluación de las acciones tomadas.

3. Comparación de estado previo a la toma de medidas y el estado actual después de la toma de medidas.

4. Capacitación enfocada a:

   a. Concienciación: Enfocada a las generalidades referentes a la protección de datos personales.
   b. Entrenamiento: Enfocado a las personas que realizan el tratamiento de información personal
   c. Educación: enfocada a impartir la cultura de la protección de la información personal dentro de la organización

V. CONCLUSIONES Y RECOMENDACIONES

- Los estándares de seguridad de la información por si solos cubren transversalmente los aspectos relacionados con la gestión de la protección de los datos personales, es por ello que las normatividades sectoriales y nacionales, entran a jugar un papel importante dentro de la adecuada gestión de la protección de los datos personales.

- Conocer las obligaciones de la normatividad relacionada a los datos personales y recurrir a una lista de chequeo de cumplimiento, no es la manera más apropiada de gestionar la seguridad de los datos personales; se requiere de un compromiso serio de las entidades, y de un marco de referencia que sirva de guía en el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de la seguridad de los datos personales, que evidencia la responsabilidad no solo de cara al cumplimiento de la ley sino del respeto por los derechos de cada individuo de la sociedad.

- La normatividad en protección de datos personales es de obligatorio cumplimiento, aplicable a organizaciones públicas y privadas de cualquier tamaño, y de cualquier sector empresarial, es por ello que un Sistema de Gestión de seguridad de Datos personales es una opción viable, que permite enfocar los esfuerzos hacia un solo objetivo, con una serie de pasos que guían el proceso de cumplimiento legal, e incorporan buenas prácticas que pueden ser medibles y comparables, abriendo la posibilidad de la mejora continua en el manejo del riesgo y gestión de la seguridad.

- La protección de datos personales debe manejarse como una labor integral, incorporando las medidas tecnológicas y administrativas, necesarias para garantizar la seguridad de los datos personales y en términos de confidencialidad, integridad y disponibilidad.

REFERENCIAS

[1]http://www.larepublica.co/asuntos-legales/las-maneras-de-cuidar-los-datos-personales_43316.
[2]http://www.sic.gov.co/drupal/recursos_user/documentos/Sentencia_C_748_2011.pdf.
[3] http://es.wikipedia.org/wiki/Informaci%C3%B3n
[4] N or m a I S O / I E C 2 7 0 0 1 : 2 0 0 5 .
[5] Guía para implementación de un Sistema de Gestión de Seguridad de Datos Personales propuesto por el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) de México.
[6] Ley 1266 de 2009.
[7] Ley 1581 de 2012.
[8] Decreto 1377 de 2013.
[9] Decreto 886 de 2014.
[10] Constitución Política de Colombia.
[11] www.engestion.com.
[12] www.sic.gov.co