INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

DEFINICON DE UN MODELO DE GESTION INTEGRAL PARA LA PROTECCION DE DATOS LEY 1581 DE 2012

JOHN MANUEL PARDO PEDREROS
Código: 1522010925

ASESOR TEMÁTICO:
WILMAR JAIMES FERNANDEZ

MAYO 2018

INDICE GENERAL

INDICE DE TABLAS

Pág.

INDICE DE FIGURAS

Pág.

RESUMEN

La criticidad y complejidad de los sistemas informáticos o de información dentro de las diferentes empresas de nuestro país hacen que las organizaciones sean más sensibles ante las amenazas presentes en el entorno. Ante esta realidad hemos visto la necesidad de buscar soluciones que obedezcan a estrategias que permitan proteger la información que estas administran o manipulan; los datos personales almacenados las base de datos o libros de Excel que permitan realizar operaciones, tales como la recolección de información, almacenamiento de esta y uso parte de las entidades.

Esta situación nos conlleva a realizar un proyecto de consultoría y asesoramiento especializado en Seguridad de la Información donde se definen actividades para acompañar a las empresas en el objetivo de definir un modelo operativo para la gestión y cumplimiento de los requerimientos normativos establecidos por la Ley 1581 de 2012; este modelo permitirá a las organizaciones revisar y determinar el uso de los datos dentro de los sistemas de información y diseñar políticas de seguridad y determinar los controles del manejo de la información, como entidad responsable del tratamiento.

PALABRAS CLAVE

Habeas Data
Decretos
Tratamiento

ABSTRACT

The criticality of information and the complexity of information systems within a company make organizations more sensitive to the threats present in the environment. Given this reality we have seen the need to seek solutions that obey strategies that protect personal data recorded in any database that allows operations, such as collection, storage, use, circulation or suppression by the Entities.

For this reason, we designed a project through the provision of consulting services and specialized advice on Information Security where activities are defined to accompany companies in order to define an operating model for the management and compliance with established regulatory requirements. by Law 1581 of 2012; This model will allow organizations to review the use of personal data contained in their information systems and rethink their policies and controls on information management, as the entity responsible for the treatment.

KEY WORDS

Habeas Data
Decrees
Treatment

INTRODUCCIÓN

En la sociedad, el uso de tecnología se convirtió en una de las actividades cotidianas las 24 horas del día, donde se mueve un volumen de información enorme desde una consulta a un sitio en internet o desde una aplicación descargada desde nuestro teléfono móvil, dando uso a ilimitados servicios donde se entrega una información sensible de una persona o una entidad, de esto nace una preocupación sobre los derechos fundamentales de las personas; algo conocido como el Habeas Data y/o ley de protección de los datos.

En Colombia se reglamentó una la ley denominada Ley 1581 de 2012; esta genero un movimiento que dio gran importancia a la protección de la información enfocado en los datos personales. Se busca que toda organización adopte las buenas prácticas y procedimientos establecidos para el procesamiento de la información de una forma adecuada que permita cumplir las normas establecidas por la ley en busca de dar un buen uso y un manejo correcto a la información de las personas, entidades y terceros que este almacenada de alguna forma dentro de los diferentes sistemas de una organización.

DESCRIPCIÓN SITUACION DEL PROBELMA

De acuerdo con el decreto reglamentario de la Ley 1581, donde la superintendencia de industria y comercio puede requerir en cualquier momento por parte de las organizaciones, el detalle de cuáles son los procesos y los procedimientos determinados para la trata de la información o datos personales que se encuentran bajo su responsabilidad; de igual forma puede exigir la implementación de políticas internas efectivas frente al tratamiento de toda la información personal que se encuentre en poder de las mismas. ¿Cuál es el modelo a seguir para cumplir con este requerimiento?

JUSTIFICACIÓN

La implementación y desarrollo de un modelo integral que permita la gestión de datos personales en una organización busca cumplir a cabalidad lo estipulado por la ley 1581 de 2012, alineándose con la guía de implementación del principio de responsabilidad demostrada y definida por la superintendencia de industria y comercio (SIC), permitiendo a las entidades responsables del tratamiento de la información demostrar y asegurar ante los titulares de los datos y la SIC una debida diligencia en el tratamiento de datos personales.

Contar con estas medidas ayuda a las organizaciones a mitigar riesgos, permitiendo ofrecer una mayor confianza ante sus clientes y proveedores, maximizar su reputación y evitar multas, sanciones o bloqueos de las bases de datos por parte del ente de control.

Figura 1. Guía SIC

"En 2014, la Superintendencia de Industria y Comercio (SIC) impuso multas por un valor total de $1.892 millones a 46 empresas que violaron el Habeas Data (protección de datos personales). Se presentaron además 4.889 quejas y se impartieron 153 órdenes administrativas de eliminación, corrección o actualización de información en bases de datos". (Prado, 2015)

Las sanciones estipuladas superan los 2.000 salarios mínimos legales vigentes y pueden ordenar un cierre temporal o en el peor de los casos definitivo de un la empresa.

OBJETIVOS

OBJETIVOS GENERAL

Definir un modelo integral de gestión de datos personales en busca del cumplimiento lo estipulado por la ley 1581 de 2012 y los decretos establecidos.

OBJETIVOS ESPECÍFICOS

- Asesorar y proponer un modelo que permita a la empresa cumplir la ley de protección de datos 1581.

- Determinar lineamientos y procedimientos que permitan mitigar los riesgos y consecuencias de las brechas de los datos.

ALCANDE DEL PROYECTO

Implementar todas y cada una de las medidas de carácter legal para alcanzar el cumplimiento de la ley y asegurar desde el punto de vista jurídico los procesos donde se involucre información clasificada como personal. Los procesos sobre los cuales se realizará la identificación son los siguientes:

- El Inventario de bases de datos
- La definición de la política para el tratamiento de información
- Definición de la metodología de gestión de riesgos asociados al tratamiento de datos personales.
- La definición de los procedimientos de seguridad según aplique:
    - Procedimientos de control de acceso lógico a la información de la organización.
    - Control de acceso físico.
    - Gestión de copias de respaldo de la información.
    - Gestión de cambios (procedimientos)
    - Administración de software

    - Identificación de la legislación aplicable
    - Gestión de terceros
    - Transferencia de información
    - Eliminación segura de información.
    - Protección de la información contra malware.
    - Gestión de seguridad en redes
    - Mantenimiento reutilización y baja o retiro de equipos.
    - Medidas disciplinarias
    - Derechos de propiedad intelectual.
- Definir una estructura organizacional.
- Definición del procedimiento de auditoria interna.
- Definición del protocolo de respuesta en el manejo de Incidentes.
- Definición de responsabilidades de gestión del tratamiento en las transferencias y/o transferencias internacionales.
- Definición del procedimiento de comunicación externa.
- Definición del procedimiento de evaluación y revisión continúa de los procesos.
- Las bases de datos a tener en cuenta son:
    - Empleados activos y Empelados retirados.
    - Clientes y proveedores de la organización.
    - Visitantes

REVISIÓN DE LITERATURA / ANTECEDENTE

Las organizaciones de nuestro país deben cumplir con la normatividad impuesta sobre la protección de datos donde deben establecer mecanismos que permitan desarrollar este objetivo de manera óptima para esto es necesario elaborar un método integral que permita abordar la protección de datos de manera efectiva que nos lleve a cumplir con las regulaciones de forma eficiente y certera, Para así minimizar los riesgos y consecuencias que se presentan con las brechas de datos que se presentan frente a manejo de protección de datos para dar cumplimiento a las normas estipuladas.

MARCO LEGAL

La implementación de medidas de carácter legal para alcanzar el cumplimiento de la ley involucra información de tipo personal señaladas en la normatividad. Es un derecho constitucional fundamental que le permite a todo individuo saber, conocer, actualizar y confirmar o modificar la información que las entidades o terceros tengan en su poder tales como archivos y bancos de datos; este derecho está incluido en la **Constitución Política de Colombia bajo el artículo (15**), el cual establece que “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 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”. (Constitucional, 2016)

Ley 1266 de 2008, regula el manejo de la información almacenada en las bases de datos personales, especialmente en el sector financiero, y la información que se origina de países, es decir la historia crediticia de las personas. Es importante tener en cuenta que la ley 1266 de 2008 se limitó exclusivamente a regular el denominado **hábeas data financiero**.

Ley estatutaria 1581 de 2012, en el artículo 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios: f) Principio de acceso y circulación restringida, g) Principio de seguridad, h) Principio de confidencialidad. (162)

(Republica, 2018)

Decretos Reglamentarios 1727 de 2009. Determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

METODOLOGIAS EXISTENTES

La ley de protección de datos personales busca resguardar y/o proteger el derecho que tienen todas las personas a conocer, modificar y actualizar toda información que esté almacenada en los diferentes sistemas de las entidades públicas o privadas.

La súper intendencia define una guía de formatos modelo para el tratamiento de datos personales bajo la ley 1581 de 2012.

Donde definen bajo cuales parámetros se hace obligatorio la autorización al tratamiento y la clasificación del dato, Dando las pautas para orientar de qué forma

se debe obtener autorización por parte del dueño o del titular para que sus información sea tratada y anexa un esquema base de los documentos a implementar, como la autorización del tratamiento de datos y el aviso de la privacidad de los mismos.

La guía de implementación plantea una serie de pasos para su implementación dentro de un sistema de gestión; desde el análisis de los diferentes procedimientos establecidos para la agrupación de datos al inventario de las bases de datos donde se concentra la información personal; planteado en cinco fases para su elaboración: fase de diagnóstico, fase de adecuación, fase de implementación y fase de revisión.

ESTRATEGIA METODOLOGICA

METODOLOGÍA DE GESTIÓN DE RIESGOS

Se definirá e implementará la metodología de gestión de riesgos asociados al tratamiento de datos personales alineado a las mejores prácticas definidas en la Norma ISO 31000, cubriendo la totalidad de las bases de datos identificadas durante la etapa anterior.

Como resultado del ejercicio se tendrá lo siguiente:

- Listado de riesgos asociados a las bases de datos identificadas.
- Definición del plan de tratamiento que permita identificar las acciones apropiadas, los elementos, responsabilidades, recursos humanos y la prioridad para manejar y controlar los diferentes riesgos identificados dentro de las bases de datos.

La metodología utiliza como base el modelo PHVA con el objetivo de establecer un proceso de gestión que lo lleve a una mejora continua.

PLANIFICAR >>>HACER>>>VERIFICAR>>>ACTUAR

Un riesgo es definido como una “pposibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias”. (Departamento Nacional de Planeación. CONPES 3854, 2016)

La gestión del riesgo busca identificar y determinar los controles que permitan otorgar que la información contenga confidencialidad, integridad y la disponibilidad de los datos de las organizaciones.

Dentro de los riesgos encontramos los siguientes:

- ✓ **Fuga de la Información**
- ✓ **Pérdida de la confidencialidad, integridad y disponibilidad.**

La metodología planteada para establecer el nivel de implementación de los controles aplicados en la Organización sobre las bases de datos o archivos que permita cumplir los requisitos establecidos por la ley 1581; la organización y/o sus clientes internos y externos.

Está basada en las mejores prácticas y cubre las siguientes fases:

- Planeación
- Ejecución (definición del modelo)
- Seguimiento y Control
- Cierre

De esta forma se llevara a cabo las fases para el desarrollo de la metodología de forma integral.

DESARROLLO E IMPLEMENTACION

PLANEACIÓN DEL PROYECTO

La fase de Planeación del Proyecto tiene como propósito establecer el esfuerzo requerido para lograr los objetivos del mismo. En esta fase se establecen las actividades a desarrollar con el fin de garantizar el éxito del proyecto.

EJECUCION DEL PROYECTO

CONOCIMIENTO DE LA ORGANIZACIÓN

Esta fase contempla el entendimiento del negocio de la organización, haciendo énfasis en los procesos que hacen parte del alcance del SGSI, de tal manera que se pueda identificar:

- Misión y visión de la organización
- Lineamientos estratégicos de negocio
- Requerimientos legales y regulatorios
- Identificación objetivos de seguridad
- Cadena de valor productos y servicios ofrecidos
- Identificación de los diferentes procesos y áreas en las que se recolecta y gestiona información personal
- Requerimientos de privacidad de la información los cuales pueden provenir de políticas internas, necesidades del negocio y/o requerimientos legales.
- Actores relevantes en el flujo de la información
- Otros

DEFINICIÓN DEL MODELO DE GESTIÓN INTEGRAL PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

INDUCCIÓN A LA LEY 1581.

Previo al inicio de las actividades del proyecto se realizará una inducción a los líderes de las gerencias participantes, sobre los aspectos generales de la Ley

1581 de 2012, con el fin de lograr que los participantes del proyecto conozcan la misma y de esta forma participen activamente en la ejecución del proyecto.

Una vez finalizada la inducción, se entregarán las plantillas sobre las cuales se realizará el respectivo levantamiento de información de las diferentes sistemas de almacenamiento de datos encontradas para iniciar el proceso de identificación de las mismas.

IDENTIFICACIÓN DE LAS BASES DE DATOS PERSONALES

Durante esta fase del proyecto se busca identificar la información de carácter personal de empleados, retirados, clientes, proveedores y visitantes que es recolectada y gestionada por la empresa cliente y que, en caso de pérdida, compromiso, o divulgación no autorizada, podría causar un daño sustancial, afectar la intimidad o discriminación de los propietarios de la misma.

DEFINICIÓN DEL MODELO

Durante esta fase se procederá a definir el modelo gestión integral.

Para la definición del modelo de gestión se tomará como marco de referencia el estándar ISO 27001:2013 y el anexo a – ISO 27002:2013.

El modelo estará compuesto por políticas y procedimientos para una adecuada gestión y cumplimiento de la normatividad.

Las consideraciones de seguridad a tener en cuenta, entre otras, son:

- Manual para la gestión del modelo.
- Política para la protección de los datos personales

- Protocolos para la respuesta y control de incidentes
- Responsabilidades de gestión por parte del personal encargado de las transferencias y/o internacionales de datos personales
- Procedimientos de Comunicación Externa
- Procedimiento de Evaluación y Revisión Continua
- Procedimientos de Auditorías Internas
- Procedimientos de Acciones Correctivas Procedimientos de Control de Documentos y Registros

DIVULGACIÓN o SOCIALIZACION

Durante todas las etapas del proyecto se realizará la divulgación de las políticas y los diferentes procedimientos establecidos a los responsables de la ejecución de estas actividades, con el fin de que se proceda con la implementación y generación de evidencias que permitan sustentar el cumplimiento con los requisitos tanto de la ley como del modelo establecido.

SEGUIMIENTO Y CONTROL DEL PROYECTO

Esta fase tiene como propósito monitorear la elaboración y el desarrollo del proyecto con el propósito de dar cumplimiento a los objetivos propuestos durante la fase de planeación y de esta manera tomar oportunamente los controles o medidas necesarias en caso de detectarse o identificar desviaciones en su ejecución.

El desarrollo de esta fase está a cargo del Líder del Proyecto, generando las evidencias del seguimiento y control: Actas, informes de seguimiento, entre otros.

CIERRE DEL PROYECTO

Con las actividades de esta fase se busca cerrar formalmente el proyecto o una fase del mismo. Adicionalmente, se verifica el estado final de los entregables del

proyecto con el objeto de formalizar su aceptación a satisfacción por parte del cliente y asegurar el cumplimiento de los compromisos contractuales.

RESULTADOS

La definición del modelo de gestión para de la protección de datos de acuerdo a la metodología implementada generará algunos entregables para la organización lo cual hará parte de los lineamientos a tomar para la conservación y mantenimiento del sistema; donde se tendrán:

Documento de la introducción o inducción a la Ley 1581 de 2012, para la divulgación en la empresa y sus usuarios.

Inventario de los sistemas de almacenamiento y bases de datos: Entregable del inventario de las bases de datos e información sujeta a protección.

Metodología de gestión de riesgos: definición del plan para el tratamiento de los riesgos y mitigar efectivamente los riesgos clasificados.

Definición del Modelo para la protección de datos personales, incluyendo las políticas y procedimientos.

DISCUSIÓN Y CONCLUSIONES

Para el desarrollo de este modelo de gestión es necesario que las organizaciones dispongan del personal idóneo para el desarrollo de las actividades.

El cumplimiento del cronograma de actividades es fundamental para el desarrollo del proyecto para así lograr entregar los informes y/o entregables de manera oportuna.

La participación del personal de la organización es importante para el desarrollo de los compromisos propuestos en las diferentes fases del proyecto ya sea entrega de información o entrevistas.

El avance de cada fase debe generar un entregable o informe el cual debe ser avalado por el líder del proyecto y la dirección de la organización o el representante de la misma.

REFERENCIAS

162, T. (s.f.). *LEGAL LEGIS.* Obtenido de LEGAL LEGIS: http://legal.legis.com.co/document.legis/tutela-162?contexto=rtutela_db221a5245ea0088e0430a0101510088&documento=rtutela&vista=STD-PC

Constitucional, C. (28 de Septiembre de 2016). *Corte Constitucional.* Obtenido de http://www.corteconstitucional.gov.co: http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

Departamento Nacional de Planeación. CONPES 3854, p. 2. (11 de Abril de 2016). *Departamento Nacional de Planeación. CONPES 3854, pág 24.* Obtenido de www.dnp.gov.co: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Prado, J. R. (07 de Marzo de 2015). *La Republica*. Obtenido de www.larepublica.co: http://www.larepublica.co/la-violaci%C3%B3n-de-habeas-data-dej%C3%B3-multas-por-1892-millones-durante-el-a%C3%B1o-pasado_228696

Público, M. d. (15 de Mayo de 2009). *Decreto_1727_de_2009 – Ministerio de Hacienda y Crédito Público.* Obtenido de www.alcaldiabogota.gov.co: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36251

Republica, C. d. (27 de Febrero de 2018). *Secretaria Senado*. Obtenido de www.secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html