DEPARTAMENTO DEL VALLE DEL CAUCA
GOBERNACIÓN
Secretaría de las Tecnologías de la Información y las Comunicaciones

Marco Arnulfo Peña
08-09-2016
2:51 PM

0400-25 265380

Santiago de Cali, 07 de septiembre de 2016.

Doctora
NORMA HURTADO SANCHEZ
Secretaria General
Presente

Asunto: Política de seguridad de la información y protección de datos personales

Cordial saludo,

En respuesta al oficio No. 060-25 265380, para el asunto de seguridad de la información y protección de datos personales, me permito comunicarle lo siguiente. Este tema ha tomado una relevancia insospechada desde hace unos años, dicha importancia se debe a la relación directa que existe entre el crecimiento tecnológico, la necesidad y dependencia de datos y tecnologías de la información por parte de personas y procesos productivos en las organizaciones.

La Ley 1581 de 2012 de protección de datos personales y su decreto reglamentario 1377 incorporan en Colombia el principio de responsabilidad demostrada o ACCOUNTABILITY, el cual consiste en la obligación que tiene todo responsable del tratamiento de datos personales, de demostrar que ha implementado un plan de gestión integral de datos personales que cumple por lo menos con los siguientes requisitos:

- Comprometer a la alta dirección y se deben asignar responsabilidades al interior de la organización.
- Presentar informes que reflejen el estado de cumplimiento de la norma.
- Implementar procedimientos operacionales (documentar procesos de tratamiento de información, ejemplo: Hacienda, Pasaportes, Tecnología, etc).
- Elaborar un inventario de bases de datos (conocer los datos personales que se almacenan de acuerdo a las finalidades de recolección).
- Elaborar políticas internas efectivas (Desarrollar e implementar procedimientos administrativos, procedimientos, lineamientos).
- Implementar un sistema de administración de riesgos asociados al tratamiento.

- Formar y educar a colaboradores.
- Establecer protocolos de respuesta en el manejo de violación de incidentes.
- Regulación contractual de los encargados del tratamiento en transmisión y transferencia de datos.
- Comunicar de forma externa cambios en las políticas, autorizaciones, etc.

El derecho a la protección de los datos personales es un derecho de tipo fundamental, pero a pesar de esto, hoy en día enfrentamos constantes irregularidades tanto en la toma de los datos, como en las operaciones, procedimientos de tratamiento y conservación de los datos de las personas naturales y jurídicas.

Es común que todas las organizaciones utilicen información personal en distintos procesos para el desarrollo de su actividad, en su día a día recoge datos personales, de forma verbal, y escrita, a través de sus portales web, correo electrónico, formularios físicos; desconociendo en muchas ocasiones que dichos datos y su posterior tratamiento debe cumplir con las disposiciones legales en materia de manejo, procesamiento, almacenamiento y uso de las bases de datos.

Es necesario y obligatorio en términos de la Ley 1581 de 2012 y sus decretos reglamentarios, adoptar medidas legales y técnicas necesarias para cubrir posibles contingencias que se generen en el tratamiento de este tipo de datos y el riesgo de que los mismos puedan ser filtrados, perdidos o hurtados, lo que podría generar responsabilidad a las organizaciones por ser estas responsables o encargadas de los datos.

Con base a todo lo anterior, la Secretaría de las Tecnologías de la Información y las Comunicaciones del Valle del Cauca ha venido trabajando en el diseño de una metodología y unas políticas de protección de la información en la Gobernación del Valle, de acuerdo a un proyecto organizado en 3 fases.

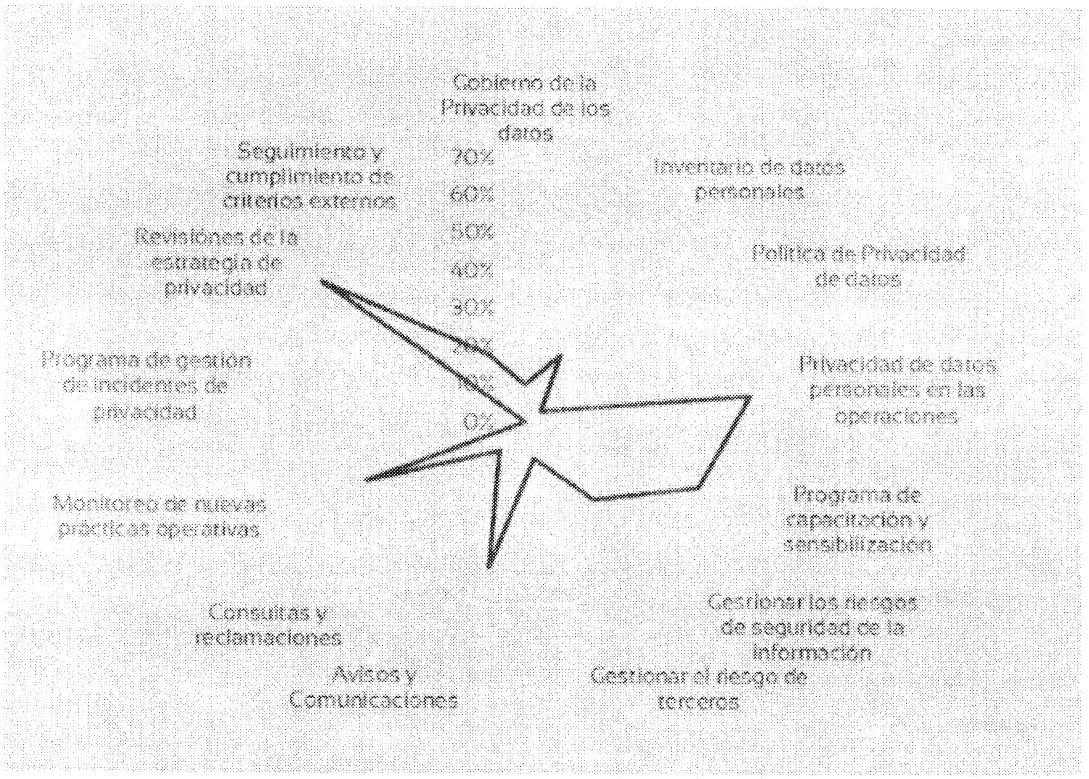
FASE 1: ENTENDIMIENTO

Determinar el contexto estratégico

- Inventario de los sistemas de gestión existentes
- Requisitos legales, reglamentarios y contractuales
- Infraestructura de TI
- Instalaciones físicas
- Sesiones con directivos y dueños de procesos

- Arquitectura Empresarial (Adoptada del Modelo IT4+ del gobierno Nacional

Con base en estas actividades se realiza un análisis GAP que determina el cumplimiento de la Gobernación en los siguientes elementos sobre un porcentaje de 0 – 100%



Los resultados que arroje el análisis GAP se procederá a las siguientes fases:

FASE 2: DISEÑO

Consiste en diseñar:

- Un sistema de gestión de datos personales
- La estrategia de privacidad
- El programa de sensibilización en privacidad
- Indicadores de gestión
- Caracterización de procesos
- Procesos de control documental

- Mecanismo de auditoría interna

FASE 3: EJECUCIÓN DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES
Comprende:

- Política de Protección de datos personales
- Objetivos e indicadores
- Procedimientos de revisión y mejora continua

Igualmente se debe desarrollar un programa de Gestión de Riesgos de Privacidad que comprende:

- Metodología para la gestión del riesgo
- Mapa de riesgos
- Plan de tratamiento de los riesgos

Algunas de las actividades que se deben desarrollar en el programa son:

- Definición de roles y responsabilidades
- Inventario de bases de datos personales
- Procedimientos de recolección, uso y destrucción de datos personales
- Programa de sensibilización
- Procedimientos para la gestión de riesgos de seguridad de la información
- Avisos de privacidad
- Procedimientos para el ejercicio de los derechos
- Procedimiento para la gestión de incidentes

OBJETIVOS ESPECÍFICOS DEL PROYECTO

- Establecer un contexto estratégico que permita apoyar el diseño, desarrollo y gestión de la estrategia de protección de datos personales.
- Desarrollar los procedimientos y documentación requeridos para la gestión del Sistema de Gestión de protección de datos.
- Establecer los criterios y lineamientos que se deben seguir para la administración de los riesgos de privacidad, de manera que se apoye el cumplimiento de los objetivos estratégicos de la Gobernación.
- Diseñar un programa de sensibilización en privacidad que permita generar entendimiento de la importancia de la protección de datos en de la organización.
- Establecer los controles requeridos para mitigar los riesgos de privacidad.

METODOLOGIA

Construir el documento de seguridad con todas las medidas técnicas y organizativas de la Gobernación, en el cual se redactarán las revisiones de seguridad realizadas y se realizará el informe con las recomendaciones técnicas.

El documento de seguridad estará alineado con el estándar ISO/IEC 27001 :2013 que contiene los siguientes elementos:

MATERIA	MEDIDAS DE SEGURIDAD
Responsable de Seguridad	Designar en el área de Gestión de TI dos responsables de seguridad (encargados de coordinar y controlar las medidas del documento.)
Personal	Definición de funciones y obligaciones de los usuarios, autorizaciones delegadas, formación de los usuarios.
Incidencias	Registro de incidencias. Procedimiento de notificación y gestión
	Anotar procedimientos de recuperación, persona que ejecuta y datos restaurados. Autorización del responsable para recuperación.
Control de Accesos	Relación de usuarios. Controles de acceso. Mecanismos que eviten el acceso no permitido. Concesión de permisos por personal autorizado. Mismas condiciones para personal ajeno.
	Control de acceso físico a los locales
	Registro de accesos. Revisión mensual del registro por el responsable de seguridad.
	Control de accesos autorizados. Identificación accesos a documentos accesibles por varios usuarios.
Identificación Autenticación	Identificación y autenticación personalizada.
	Asignación, distribución y almacenamiento ininteligible de contraseñas.
Periodicidad del cambio.	Límite de intentos reiterados de acceso no autorizado. Inventario de soporte. Identificación de información que contiene. Autorización de salidas en soportes. Medidas para el transporte y desechado.

Gestión de Soportes	Registro de entrada y salida de soportes. Sistema de etiquetado confidencial. Cifrado de datos en la distribución. Cifrado de información en soportes portátiles fuera de las instalaciones.
Copia de Respaldo	Procedimiento de copia y recuperación. Verificación semestral. Reconstrucción de datos a partir de la última copia. Pruebas con datos reales. Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos
Criterios de archivo	Realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de derechos.
Almacenamiento	Se manejara indicadores de Estadísticos de data, capacidad.
Custodia de soportes	Diligencia de los usuarios durante la custodia y transporte de los documentos para evitar accesos no autorizados.
Copia o reproducción	Control con procedimientos y herramientas de la informacion

Atentamente,

FRANK ALEXANDER RAMIREZ ORDÓÑEZ
Secretario de las Tecnologías de la Información y la Comunicaciones

Redactor y transcriptor: Ing. Oscar Julio Molano Díaz – Coordinador de Gestión TI