ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

2019

TABLA DE CONTENIDO

1. *INTRODUCCION*

Las tendencias tecnológicas de los últimos años, han permitido crear de manera exponencial cantidades de información que jamás en la historia de la humanidad se habían creado, transportado, transformado o compartido, cambiando tanto la manera de ver las cosas por parte de todos nosotros. Particularmente en las entidades del estado, se hace necesario contar con la conciencia del poder de la información, el alcance que tiene la misma y principalmente la entrega oportuna que se debe dar a la ciudadanía.

En la Secretaría de Seguridad, Convivencia y Justicia se cuenta con gran volumen de información, relevante para el Distrito, manejada física, digital y electrónicamente, en su mayoría con el propósito de dar cumplimiento a los objetivos de la entidad, requiriendo utilizar mecanismos adecuados para cuidar el derecho a la intimidad personal, familiar y al buen nombre de todos los beneficiarios de la entidad, permitiendo el acceso a los documentos públicos y evitando el acceso a los que se consideren reservados o confidenciales.

Para lograr la toma de decisiones con base en información de altos estándares de calidad, en materia de política y gestión de Seguridad, Convivencia y Acceso a la Justicia, que permita tomar decisiones, resolver problemas y prestar los servicios a los ciudadanos y funcionarios de la entidad, es necesario que esta sea real, oportuna y de acceso a las personas o procesos que lo requieren.

Teniendo en cuenta lo anterior, en el marco internacional, la norma ISO 27001 ayuda a establecer un Sistema de Gestión de Seguridad de la Información que permite convertir las necesidades propias de la información en una ventaja frente al cumplimiento de la normativa legal vigente y las mejoras en la prestación de los servicios en cualquier organización pública o privada, permitiendo desarrollar procesos medibles que cumplan un objetivo alineado con los de la entidad, optimizando de este modo el rendimiento de las áreas, teniendo en cuenta aspectos físicos, legales, interacción con terceros, hasta la continuidad de la prestación de los servicios tecnológicos y manuales, todo en acompañamiento de validaciones externas que permitan mejorar el rendimiento de las metas establecidas.

Basado en la norma ISO27001 y los requisitos legales, la Secretaría de Seguridad, Convivencia y Acceso a la Justicia, establece un plan para el año 2019 que permite crear las bases para el cuidado continúo de la información en la organización, a través de controles, procedimientos, definición de responsables, partes interesadas, actividades de medición y cumplimiento de estos con el fin de dar cumplimiento a la política de Seguridad de la Información.

2. OBJETIVOS

Objetivo General

Definir el plan de actividades para proteger la información física, digital y electrónica que almacena, recolecta, produce y gestiona la Secretaría de Seguridad, Convivencia y Justicia a través de la implementación de controles físicos y lógicos, gestión de riesgos y la mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

Objetivos Específicos

El Plan de Seguridad y Privacidad de la Información da cumplimiento al objetivo general a través de los siguientes objetivos específicos:

1. Establecer lineamiento para el cumplimiento de la Política de Seguridad de la Información en la secretaría.
2. Identificar los activos de información de la entidad.
3. Identificar los riesgos de seguridad digital de la entidad que puedan afectar la confidencialidad, integridad y disponibilidad de la información en el entorno digital.
4. Establecer actividades de concienciación sobre Seguridad de la Información.

3. GLOSARIO DE TÉRMINOS

- **Activo de información:** se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la entidad. (Sistemas, soportes, edificios, hardware, recurso humano).

    - Datos: Corresponde a los elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la SDSCJ.
    - Aplicaciones: Corresponde al software que se utiliza para la gestión de la información.
    - Personal: Corresponde a todo el personal de la SDSCJ, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la SDSCJ.
    - Servicios: Corresponde a los servicios internos, suministrados al interior de la entidad o servicios externos; suministrados por la entidad a un tercero; cliente o usuarios
    - Tecnología: Corresponde a los equipos utilizados para gestionar la información y las comunicaciones.
    - Instalaciones: Corresponde a todos los lugares en los que se aloja información de la entidad.
- **Amenaza**: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis de riesgos:** uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.
- **Backup o copia de seguridad:** copia de respaldo de la información.
- **Confidencialidad:** propiedad que garantiza que la información no sea accedida, ni sea revelada a personas, entidades o procesos no autorizados.
- **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas; y que pueden ser de carácter administrativo, técnico o legal.
- **Criticidad**: medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.
- **Custodio**: ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.
- **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma
- **Disponibilidad**: principio que garantiza que la información esté accesible y utilizable cuando lo requieran las personas, entidades o procesos autorizadosEquipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y

ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

- **Encriptación**: Proceso que permite volver ilegible la información que se considera importante. Una vez la información esta encriptada solo puede accederse aplicando una clave.
- **Evaluación de riesgos:** Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento de seguridad de la información:** situación detectada en un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información de la entidad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Impacto**: Resultado de un incidente de seguridad de la información.
- **Incidente de seguridad de la información**: es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información, tales como, un acceso no autorizado o intento del mismo; uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos
- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.
- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Principios de Seguridad de la información:** confidencialidad, disponibilidad e

integridad.

- **Propietario/responsable de la información:** individuo, entidad o unidad de negocio que tienen bajo su responsabilidad la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- **Seguridad de la Información:** consiste en resguardar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la entidad, mediante un conjunto de medidas preventivas y correctivas.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4. MARCO LEGAL

- **Artículo 15 De La Constitución Política De Colombia:** se establece que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el estado 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 los archivos de entidades públicas y privadas".
- **Ley 1581 De 2012:** por la cual se dictan disposiciones generales para la protección de datos personales tiene como 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" y que dicta, además de las disposiciones generales para la protección de datos personales.
- **Decreto 1377 De 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012" y se dictan disposiciones generales para la protección de datos personales.
- **Decreto 886 de 2014:** Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- **Ley 1712 De 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Conpes 3854 de 2016:** Política nacional de seguridad digital
- **Resolución 541 de 2017**: Por la cual se adopta la política de seguridad de la información en la SDSCJ y se definen lineamientos para su uso, actualización y aplicación.
- **Resolución 645 de 2018**: Por la cual se adopta la política de protección de datos personales de la SDSCJ.

- **Decreto 1008 de 2018**: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del Decreto 1078 de 2015 , Decreto Único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones

5. *CRONOGRAMA DE IMPLEMENTACIÓN PLAN DE SEGURIDAD DE LA INFORMACIÓN - 2019*

Continuando con el proceso de implementación del Sistema de Gestión de Seguridad de la Información en la Secretaría de Seguridad, Convivencia y Justicia, el plan de Seguridad y Privacidad de la Información establece las actividades que permitan incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

A continuación, se describen las actividades para desarrollar en la vigencia del 2019 en toda la entidad:

1. Definición de Guía para la Identificación, Clasificación y Valoración de Activos de Información
2. Elaboración del Instrumento de identificación, clasificación y valoración de activos de información
3. Identificación, clasificación y valoración de activos de la entidad
4. Elaboración del manual de seguridad de la información
5. Actualización de la Política de Seguridad de la Información
6. Definición de instrumentos de seguridad de la información
    a. Normograma
    b. Matriz de roles y responsabilidades
    c. Matriz de aplicabilidad.
    d. Procedimiento de Adquisición, Desarrollo y Mantenimiento de software. (Apoyo)
    e. Plan de Contingencia Tecnológica-DRP
    f. Procedimiento de Gestión de Cambios (Actualización).
7. Actualización de la política de administración de riesgos de la entidad, incluyendo riesgos de seguridad digital.
8. Elaboración del instrumento de identificación y clasificación de riesgos digitales
9. Identificación, clasificación de riesgos digitales en la entidad.
10. Definición del plan de Concienciación en seguridad de la información en la entidad

11.Definición de indicadores de seguridad de la información.
12.Registro Nacional de Bases de Datos ante la SIC

Estas actividades se realizarán hasta diciembre de 2019 en el siguiente orden:

N°	Nombre Tarea	2019											
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	**Guía para la Identificación, Clasificación y Valoración de Activos de Información**												
1	Definir Guía de Activos de Información												
2	**Instrumento de identificación, clasificación y valoración de activos de información**												
1	Elaborar Instrumento de Activos de Información												
3	**Identificación, clasificación y valoración de activos de información la entidad**												
1	Identificar, clasificar y valorar activos de información en la entidad												
4	**Manual de Seguridad de la Información**												
1	Elaborar manual de seguridad de la información												
5	**Política de Seguridad de la Información**												
1	Actualización Política de seguridad de la información												
6	**Instrumentos de seguridad de la información**												
1	Elaborar Normograma de TIC												
2	Elaborar Matriz de roles y responsabilidades												
3	Elaborar Matriz de Aplicabilidad												
4	Apoyar la elaboración del procedimiento de Adquisición, desarrollo y mantenimiento de software												
5	Elaborar plan de contingencia tecnológica-DRP												
6	Actualización Procedimiento Gestión de Cambios												
7	**Política de Administración de Riesgos de SDSCJ – Riesgos de Seguridad Digital**												
1	Actualizar Política de Riesgos												
8	**Instrumento de Riesgos de Seguridad Digital**												

N°	Nombre Tarea	2019											
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	Elaborar Instrumento de Riesgos												
9	**Identificación, Clasificación de riesgos digitales en la entidad**												
1	Identificar y clasificar riesgos de seguridad digital												
10	**Plan de Concienciación en Seguridad de la Información**												
1	Enviar Boletines de Seguridad de la Información												
2	Realizar Charlas de Seguridad de la Información												
11	**Indicadores de Seguridad de la Información**												
1	Definir indicadores de seguridad de la información												
12	**Registro Nacional de Bases de Datos**												
1	Realizar el Registro Nacional de Bases de Datos ante la SIC												

6. CONTROL DE CAMBIOS

Control de Cambios		
Fecha	**Versión**	**Descripción**
23/07/2018	1	Creación del documento.
12/08/2019	2	Actualización de contenidos en: Glosario de Términos; inclusión de términos Marco Legal; inclusión de normas Cronograma de Implementación de acuerdo a plan de trabajo 2019

Firma de Autorizaciones					
ELABORÓ		**REVISÓ**		**APROBÓ**	
Nombre(s):	Lourdes María Acuña Acuña	**Nombre(s):**	Diego Ferney Ramírez Pulido	**Nombre(s):**	Andrés Javier Solorzano Ulloa
Firma (s):		**Firma (s):**		**Firma (s):**	
Cargo (s):	Contratista	**Cargo (s):**	Contratista	**Cargo (s):**	Director de Tecnología y Sistemas de Información