2020

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GRUPO DE GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

1. OBJETIVO

Definir la planificación de las actividades orientadas a fortalecer el tratamiento de la información que es generada, tratada y custodiada por ENTerritorio; con el fin elevar su nivel de confianza con sus grupos de interés, mediante la preservación de su confidencialidad, integridad y disponibilidad, así como también la adopción de las buenas prácticas y el cumplimiento de la política de gobierno digital, el Modelo de Seguridad y Privacidad de la Información y el marco legal que le sea aplicable.

1.1 OBJETIVOS ESPECÍFICOS

- Fortalecer el Sistema de Gestión de Seguridad de la Información, mediante la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información.
- Apoyar el cumplimiento de los requisitos legales y normativos en materia de seguridad y privacidad de la información y protección de la información personal.
- Gestionar los riesgos de seguridad y privacidad de la información y continuidad de la operación de la Entidad de manera integral.
- Definir y divulgar las políticas, lineamientos, procedimientos y buenas prácticas recomendaciones para establecer una cultura organizacional de seguridad de la Información en la entidad.
- Realizar el seguimiento a las acciones pertinentes a reducir las brechas de cumplimiento de acuerdo con el autodiagnóstico del MIPG relacionado al habilitador transversal de seguridad y privacidad de información.
- Definir estrategias para la gestión de las vulnerabilidades técnicas en la infraestructura tecnológica y los sistemas de información de la Entidad.

2. DEFINICIONES

- **Activo de información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta, el cual tiene valor para la organización. En la Entidad se tienen contemplados los siguientes activos de información: personas, información/dato, hardware, software, redes, infraestructura y servicios.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Confidencialidad:** Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- **Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Integridad:** Garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- **Seguridad de la información:** Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su Confidencialidad, Integridad y Disponibilidad.
- **Sistema de Gestión de Seguridad y privacidad de la información**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos,

procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de la Entidad que potencialmente permite que una amenaza afecte a un activo.

3. MARCO NORMATIVO

Dentro del marco legal más relevante para justificar el presente plan de seguridad y privacidad de la información se encuentran las siguientes normas:

- **Ley 1437 de 2011, Capítulo IV**, "utilización de medios electrónicos en el procedimiento administrativo". "Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."
- **Ley 1581 de 2012**, g) Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".
- **Ley 1712 de 2014**, "principio de transparencia": "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley". **Artículo 7:** "Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten." **Título III** "Excepciones acceso a la información" "Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."
- **Circular 007 de 2018 de la Superintendencia Financiera de Colombia:** por la cual se dictan los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad.
- **Conpes 3854 de 2016**, objetivo general "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".
- **Decreto 1413 de 2007**, artículo 2.2.17.6.5, "Privacidad por diseño y por defecto": "Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales

a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador".

- **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 libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". **ARTÍCULO 2.2.9.1.1.3.** Principios. "Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".
- **Decreto 612 de 2018**, artículo 1. "Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

4. ACTIVIDADES DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El plan de implementación parta la dimensión de seguridad y privacidad de la información comprende las siguientes actividades y se le hará seguimiento mes a mes por parte del Comité Institucional de Gestión y Desempeño:

Eje Temático	Actividad	Resultados Esperados	Fecha de inicio	Fecha finalización	Responsable
Sistema de Gestión de Seguridad de la Información	1. Preauditoria al sistema de Gestión de Seguridad de la Información con base en la norma ISO27001:2013	Informe del Resultado de la Preauditoria.	15/02/2020	15/04/2020	Grupo de TI
	2. Elaboración del plan de implementación de recomendaciones de la preauditoria	Plan de implementación de recomendaciones.	16/04/2020	16/05/2020	Grupo de TI
	3. Implementación del plan de recomendaciones.	Soportes de implementación	17/05/2020	20/12/2020	Grupo de TI
	4. Auditoría interna al SGSI	Informe de auditoría interna	1/07/2020	30/07/2020	Grupo de TI
	5. Actualización del plan de implementación según resultados de auditoría interna	Documento del plan actualizado	1/08/2020	15/08/2020	Grupo de TI

Eje Temático	Actividad	Resultados Esperados	Fecha de inicio	Fecha finalización	Responsable
Gestión de Vulnerabilidades Técnicas	6. Elaboración del Plan de remediación de las vulnerabilidades técnicas encontradas durante la vigencia anterior	Documento del plan de remediación de vulnerabilidades	15/01/2020	28/02/2020	Grupo de TI
	7. Ejecución de remediación de vulnerabilidades	Soportes de las actividades de remediación	2/03/2020	30/09/2020	Grupo de TI
	8. Análisis de vulnerabilidades técnicas (interno) para verificar brechas cerradas	Informe de resultados de análisis de vulnerabilidades	2/10/2020	15/12/2020	Grupo de TI
Gestión de activos	9. Actualización de activos de información asociados al BIA	Matriz de activos de información asociados al BIA	3/02/2020	30/04/2020	Grupo de TI
	10. Definir instructivo para la identificación y clasificación de activos de información	Instructivo de identificación y clasificación de activos de información	15/01/2020	30/03/2020	Grupo de TI
	11. Identificación de activos de información de TI	Matriz de activos de información de TI	01/03/2020	30/11/2020	Grupo de TI
	12. Actualización y publicación parcial de los instrumentos de la Ley 1712 del 2014.	- Registro de activos de información actualizado -2020 - Índice de Información Clasificada y Reservada -2020	1/04/2020	20/12/2020	Grupo de TI
Protección de datos personales	13. Desarrollar el procedimiento de gestión de datos personales	Procedimiento de Gestión de Datos Personales	15/01/2020	30/03/2020	Grupo de TI
	14. Capacitación a los colaboradores en conceptos de la ley de protección de datos personales	Dos capacitaciones por parte de funcionarios de la Superintendencia de Industria y Comercio	01/02/2020 01/07/2020	30/06/2020 20/12/2020	Grupo de TI
Monitoreo y Mejora del MSPI	15. Revisión y valoración de controles de seguridad y privacidad de la información de acuerdo con el instrumento del MINTIC	Matriz de valoración del MSPI	01/02/2020 01/07/2020	30/07/2020 20/12/2020	Grupo de TI

5. SEGUIMIENTO Y EVALUACIÓN

El seguimiento del plan se realizará mensualmente por el Grupo de Planeación y Gestión de Riesgos y la evaluación se hará al final de la vigencia utilizando el instrumento del autodiagnóstico del Departamento Administrativo de la Función Pública.