2019

PLAN DE TRATAMIENTO DE RIESGOS Y DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2019

Contenido

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 y Privacidad de la Información, mediante la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información.
- 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 al autodiagnóstico del MIPG relacionado al habilitador transversal de seguridad y privacidad de información.
- Definir y gestionar los riesgos de Seguridad y Privacidad de la Información en 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 la misma, 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.
- **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.
- **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.
- **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.

3. MARCO LEGAL

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."
- **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. ANTECEDENTES

El presente plan está orientado a mejorar por medio de la implementación acciones concretas el Sistema de Gestión de Seguridad y Privacidad de la Información; los múltiples esfuerzos generados en el año 2018 han alcanzado logros en los 3 componentes del modelo (Personas, Procesos y Tecnología), entre los que se destacan:

- **Personas:**
  - Realización de sesiones de sensibilización a los colaboradores de la entidad en los temas relacionados con la seguridad y privacidad de la información.
  - Definición del programa de Cultura Organizacional de Seguridad y Privacidad de la Información.
  - Definición y oficialización del Decálogo de buenas prácticas de Seguridad y Privacidad de la Información.
  - Realización de la encuesta de percepción de Seguridad y Privacidad de la Información.
- **Procesos:**
  - Revisión y mejora de las políticas de seguridad y privacidad de la entidad.
  - Realización de diagnóstico y grado de cumplimiento de los controles de seguridad de la información alineados con la ISO 27001:2013.

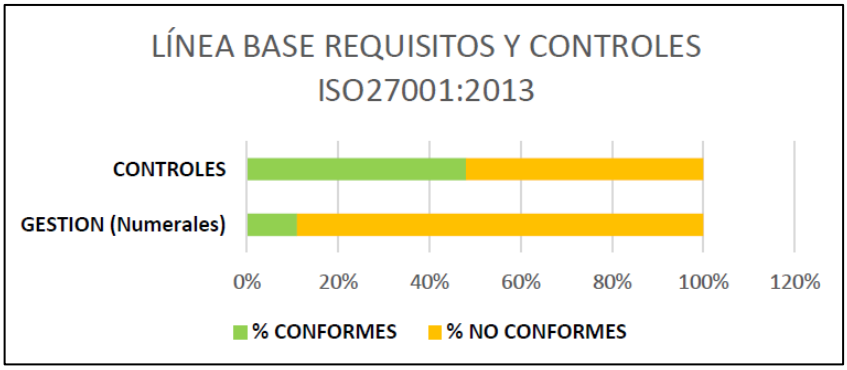

Ilustración 1. Linea Base de Requisitos y Controles de a Norma ISO 27001:2013

- **Tecnología:**
  - Definición e implementación de controles técnicos del MSPI.
  - Optimización de las herramientas tecnológicas de contención de ciberataques.

A pesar de los nombrados logros, el SGSI requiere de un proceso de mejora continua, por tal razón se contempla el siguiente capítulo de las acciones de seguridad y privacidad de la información.

5. PLANIFICACIÓN DE ACTIVIDADES

Eje Temático	Actividad	Resultados Esperados	Fecha finalización	Responsable
Categoría: Definición del marco de seguridad y privacidad de la información y de los sistemas de información				
Transición IPV4 - IPV6	1. Formulación del plan de diagnóstico y estrategia de transición de IPv4 a IPv6	- Documento de diagnóstico de transición Ipv4-Ipv6. (Hace parte de los productos del contrato de transición IPv4-IPv6)	30/09/2019	Grupo de TI
Políticas de Seguridad y Privacidad de la Información	2. Actualización de Políticas de Seguridad y Privacidad de la Información	- Manual de Políticas de Seguridad y Privacidad de la Información actualizado (*Debe ser alineado a la norma ISO 27001:2013, según recomendación de la revisión del SGSI efectuada en diciembre del 2018)*	30/07/2019	Grupo de TI
Gestión de activos	3. Actualización de los instrumentos de la Ley 1712 del 2014.	- Registro de activos de información actualizado -2019 - Índice de Información Clasificada y Reservada -2019	30/08/2019	Grupo de TI
Gestión de Riesgos de Seguridad de la Información	4. Definición de la metodología y plan de gestión de riesgos de seguridad y privacidad de la información	- Documento de metodología de gestión de riesgos de seguridad y privacidad de la información. *(Se debe integrar a la metodología de gestión de riesgos definida en la Guia del DAF de octubre del 2018)* - Definición del plan de tratamiento de riesgos de seguridad y privacidad de la información del proceso de Gestión de TI -Análisis de riesgos de seguridad y privacidad de la información del proceso de Gestión de TI	30/06/2019 30/07/2019 30/08/2019	Grupo de TI – Grupo de Planeación y Riesgos

Eje Temático	Actividad	Resultados Esperados	Fecha finalización	Responsable
	5. Definición de la declaración de aplicabilidad de acuerdo con la ISO 27001:2013	- Declaración de aplicabilidad de los controles ISO 27001:2013	15/06/2019	Grupo de TI
Categoría: Plan de seguridad y privacidad de la información y de los sistemas de información				
Planes de control operacional de seguridad de la Información	6. Establecer el plan de control operacional.	- Documento de plan de control operacional de las políticas de seguridad y privacidad de la información.	30/07/2019	Grupo de TI
Cultura organizacional en seguridad y privacidad de la información	7. Implementación del programa de Cultura Organizacional de Seguridad y Privacidad de la Información.	- Sesiones de sensibilización de seguridad y privacidad de la Información	Permanente en el año 2019	Grupo de TI
	8. Diseño, implementación y análisis de la encuesta de percepción de Seguridad y Privacidad de la Información	- 1er. Informe semestral del resultado de la encuesta de percepción de la seguridad y privacidad de la información -2do. Informe semestral del resultado de la encuesta de percepción de la seguridad y privacidad de la información	28/04/2019 29/11/2019	
Categoría: Monitoreo y mejoramiento continuo				
Monitoreo y Mejora del SGSPI y MSPI	9. Revisión y valoración de controles de seguridad y privacidad de la información de acuerdo con el Anexo A de la ISO 27001:2013	- Matriz de valoración de controles *(Corresponde a la valoración de la efectividad de los controles del anexo A de la ISO 27001:2013)*	30/08/2019 30/12/2019	Grupo de TI
	10. Medición y Reportes de indicadores del SGSI	- 1er Reporte semestral de indicadores del SGSI *(Los componentes del indicador se medirán desde febrero del 2019 y el reporte será semestral)* - 2do Reporte semestral de indicadores del SGSI	05/07/2019 05/01/2020	