PLAN DE SEGURIDAD, PRIVACIDAD Y GESTION DE RIESGOS DE LA INFORMACIÓN

Introducción. La subsecretaría general en cumplimiento de su rol como líder de la política de seguridad digital que compone el modelo integrado de planeación y gestión y acorde a lo establecido en el decreto 612 de 2018, presenta este documento para conocimiento de la ciudadanía, órganos de control y demás partes interesadas.

Objetivo y alcance del documento. Resumir los aspectos más relevantes, de las actividades que la entidad planea realizar en la vigencia 2019 y tendientes a garantizar adecuados niveles de seguridad de la información, este plan es dinámico y se ajustará acorde a las necesidades y riesgos que la entidad afronta en su día a día

Marco en el que se desarrolla este plan. En la presenta administración la entidad ha venido fortaleciendo la gestión de seguridad de la información, tomando decisiones de tipo estratégico que permitan avanzar en el logro de los objetivos, una de las decisiones fue la reubicación del rol de seguridad de la información, el cual pasó de depender de la Dirección de Informática y Tecnología a la Subsecretaría General, este enfoque alineado a las mejores prácticas en gestión de seguridad, ha permito girar hacia un enfoque estratégico y darle a la seguridad de la información el respaldo desde el más alto nivel de la organización.

En este contexto, este plan se encuentra alineado a las políticas y al manual de seguridad y privacidad de la información, resaltando los siguientes aspectos:

Políticas de seguridad y privacidad. Este documento contiene la declaración de los objetivos de seguridad, los cuales son:

- Gestionar los riesgos de seguridad de la información.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los ciudadanos, contribuyentes, entidades
- gubernamentales y servidores públicos.
- Apoyar la innovación tecnológica.
- Proteger los activos de información, como son: los datos, la infraestructura
- tecnológica y sus servicios asociados, los medios que dan soporte a la
- información e incluso las personas y sus conocimientos y habilidades.
- Establecer las políticas, estándares, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en: servidores públicos, proveedores, entes gubernamentales, ciudadanos y contribuyentes que tienen relación con la entidad.
- Disponer los mecanismos que aseguren la información, incluso durante y después de eventos de contingencia.
- Asegurar la disponibilidad de los servicios de procesamiento de información.
- Asegurar el cumplimiento de leyes y decretos aplicables, en particular los relacionados con la reserva tributaria y la protección de datos personales de: servidores públicos, contratistas y contribuyentes - cuando sea aplicable.

Por otra parte este plan, también se enmarca en las actividades consignadas en el capítulo 4 del manual del subsistema de gestión de seguridad de la información (vigente desde Mayo de 2018), documento en el cual las actividades se agrupan en tipos (o fases) así; Tipo I , agrupa los procesos existentes y que requieren algún ajuste y los procedimientos de mayor prioridad, el plazo proyectado para su implementación fue de un año contado a partir de Mayo de 2018. El estado de los procedimientos y controles agrupados en este tipo se presenta a continuación:

- Procedimiento de gestión del riesgo en seguridad de la información. Formalizado en el sistema de gestión de calidad – 76-P-02.
- Procedimiento de monitoreo de registros transaccionales: Planeado para 2019.
- Procedimiento de gestión de incidentes de seguridad y privacidad: iniciado en 2018 ya que hace parte del procedimiento 65-P-03 y en proceso de formalización.
- Procedimiento plan de continuidad de negocio. Formalizado en el sistema de gestión de calidad – 76-P-03.
- Procedimiento de administración de cuentas de usuario. Ajustado en 2018, incorporando controles para minimizar el uso no autorizado de sistemas de información.
- Procedimiento de ejecución de copias de respaldo y recuperación de información. Formalizado en el sistema de gestión de calidad – 46-P-07.
- Procedimiento de control de acceso físico. Formalizado en el sistema de gestión de calidad como instructivo adjunto al procedimiento 42-P-01.
- Procedimiento de ingreso y desvinculación del personal. Para esta vigencia se contempla la inclusión en éstos procedimiento de la firma de acuerdos

de confidencialidad y acatamiento de las políticas de seguridad y privacidad.

- Procedimiento de conservación de documentos. Formalizado en el sistema de gestión de calidad como proceso CPR-43.
- Procedimiento de gestión de vulnerabilidades. Las vulnerabilidades son gestionadas por medio del procedimiento de gestión de eventos que fue formalmente incorporado al sistema de gestión de calidad en marzo de 2018.
- Procedimiento de gestión de cambios. En este procedimiento se incorporó el rol de seguridad de la información y fue formalmente adoptado en el sistema de gestión de calidad en marzo de 2018
- Procedimiento de protección contra código malicioso. La subsecretaría en 2018, adoptó un instructivo de uso interno para el monitoreo de los eventos reportados por las herramientas antivirus con las cuales cuenta la entidad.
- Programa de gestión (protección) de datos personales. Durante la vigencia 2018 se realizó la revisión de las bases de datos sujetas a protección de datos personales, se realizó su documentación e inscripción ante la superintendencia de industria y comercio, acorde a lo establecido por la norma. Por medio de circular SDH-009-2018 por parte de la secretaria de hacienda, se impartieron lineamientos e indicaciones de las actividades que las áreas deben aplicar.

Con el estado anteriormente descrito, el plan de seguridad para la vigencia 2019, arroja las siguientes actividades:

- Monitoreo de registros transaccionales. Se retoma este procedimiento y su viabilidad bajo la plataforma SAP o apoyado en herramientas externas, especializadas.

- Gestión de incidentes: La gestión de incidentes tiene dos frentes de acción, por un lado, incorporar ajustes al procedimiento que se aplica en la subdirección de servicios de TICs, para inclusión y escalamiento de incidentes de seguridad a la subsecretaría general y por el otro, el manejo sistemático y estandarizado del tratamiento de incidentes al interior de la subsecretaría general.

- Acuerdos de confidencialidad y acatamiento de políticas. Inclusión y formalización de firma de acuerdos de confidencialidad y acatamiento de las políticas de seguridad en los procesos de contratación.

- Gestión de vulnerabilidades y protección contra código malicioso. Seguimiento y escalamiento del indicador de gestión de vulnerabilidades técnicas y eventos de código malicioso mensualmente al subsecretario y al director de informática y tecnología.

- Programa de protección de datos personales. Se contempla continuar con la sensibilización y entrenamiento en protección de datos personales, así como en seguridad de la información.

Factores internos y externos. Los factores que se presentan más adelante influyen de manera directa en el plan y su ejecución, motivo por el cual en mayor o menor grado estos darán origen a ajustes, estos son:

Factores internos. La entidad se encuentra inmersa en un proyecto de transformación digital el cual implicará cambio en procesos, actividades y tareas, de este proyecto uno de los factores que se desprende es la aparición de nuevos activos de información, los cuales por un espacio de tiempo, convivirán con los activos de información actuales, esto origina la atención y gestión de las dos plataformas.

El factor anteriormente descrito, da origen a la necesidad de realizar un análisis de riesgos sobre los nuevos activos de información, lo cual requiere el apoyo de las áreas de negocio y de soporte, actividad que está contemplada en el plan operativo de las áreas.

Factores externos. Debido a que se aproxima un cambio de administración, surge la necesidad de formalizar el equipo de seguridad de la información, lo anterior debido a que las necesidades y requerimientos de seguridad de la entidad superan lo contemplado en el manual de funciones. Esto determina que la entidad en esta vigencia debe realizar el estudio, justificación y trámite administrativo para realizar las modificaciones que se determinen.

Gestión de riesgos. En la elaboración de este plan, como se desprende de varias de las actividades ya descritas, se encuentra inmersa la gestión de riesgos, razón por la cual aquí solamente se mencionarán las actividades más relevantes que se planea realizar en 2019 y tendientes a la realización de análisis o gestión de riesgos, estas son;

- Realización de análisis de riesgos en BOGDATA (pre y post implementación)
- Definición de plan operativo con las áreas en Gobierno y Seguridad Digital.
- Gestión de incidentes
- Gestión de vulnerabilidades
- Entrenamiento y educación para el equipo de seguridad en plataforma SAP.
- Protección de datos personales, la entidad aplicará lo establecido en la circular SDH-009-2018 en cuanto a gestión de riesgos sobre datos personales.
- Revisión de exposición de información tributaria en internet.

Finalmente complementa la gestión de riesgos la necesidad de sensibilizar a la ciudadanía para minimizar el riesgo que sea víctima de fraudes en el mundo digital, razón por la cual, se planea adelantar una mini campaña con este objetivo.

Subsecretaría General
Enero 30 de 2019