SOCIEDAD DE ACTIVOS ESPECIALES

Plan de Tratamiento de Riesgos de Seguridad de la Información

Versión No. 1 – enero de 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETIVO 3

3. ÁMBITO DE APLICACIÓN 3

4. GLOSARIO 3

5. NORMATIVIDAD 5

6. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 0

6.1 Mapa de Ruta 2

1. INTRODUCCIÓN

La seguridad y privacidad de la información en las entidades tiene como objetivo la protección de cualquier tipo de activo de información ante una serie de amenazas o brechas que atenten contra los principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad y privacidad de la información, que permitan gestionar y reducir los riesgos e impactos a los cuales está expuesta la entidad y se logre alcanzar el máximo retorno de inversión con relación al cumplimiento de la misión y visión institucionales.

La Sociedad de Activos Especiales – SAE, a través de la implementación de la guía de gestión de riesgos, gestiona los riesgos de seguridad de la información con el fin de reducir su probabilidad de ocurrencia y mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la protección de los activos de información y la custodia de los datos personales de los ciudadanos.

Las actividades de valoración de riesgos, en cumplimiento del Modelo Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información MINTIC, y la política de seguridad de la información serán una herramienta para el logro de los objetivos encaminados a mantener los activos de información protegidos de amenazas internas, externas y/o deliberadas.

2. OBJETIVO

Establecer las actividades necesarias para mantener la integridad, confidencialidad, disponibilidad, trazabilidad, autenticidad, y privacidad de la información a través de la gestión de los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y Continuidad de la Sociedad de Activos Especiales – SAE.

3. ÁMBITO DE APLICACIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la información aplica a todos los procesos a nivel de Dirección General, Direcciones Territoriales y Agencias Territoriales de la entidad, donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión y cumplimiento de sus objetivos estratégicos de la SAE.

4. GLOSARIO

- **Activo de información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la entidad.

- **Administración del riesgo:** comprende el conjunto de elementos de control y sus interrelaciones, para que la entidad evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera negativa el logro de sus objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- **Amenaza:** es la causa potencial de una situación de incidente y no deseada por la organización.

- **Análisis de riesgos:** elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo.

- **Autenticidad:** Propiedad de la información que garantiza que la entidad que accede al activo está verificada y es la que declara ser.

- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Estimación del riesgo:** proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- **Evaluación de riesgos:** combinación de la probabilidad de ocurrencia de un riesgo con el impacto de su materialización, que permite determinar el grado de exposición de la entidad.

- **Evento:** un incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo específico. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

- **Impacto:** las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- **Integridad:** propiedad de la información relativa a su exactitud y completitud.

- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **Riesgo inherente:** es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Trazabilidad**: Propiedad de la información que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:** es aquella debilidad de un activo o grupo de activos de información, o de un control que puede ser explotada por una o más amenazas.

5. NORMATIVIDAD

El diseño e implementación del plan de tratamiento de riesgos de la Sociedad de Activos Especiales – SAE se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC.

- Ley 527 de 1999 del Congreso de la República. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

- Ley 1273 de 2009 del Congreso de la República. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1581 de 2012 del Congreso de la República. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1712 de 2014 del Congreso de la República. 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.

- Decreto 1377 de 2013 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 1499 de 2017 de la Presidencia de la República. Por medio de la cual se modifica el Decreto 1083 de 2015, Decreto único reglamentario de la función pública, en lo relacionado con el Sistema de Gestión establecido en el artículo de la Ley 1753 de 2015.

- Decreto 1008 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG del Departamento Administrativo de la Función Pública, marzo de 2021.

- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones.

- NTC-ISO/IEC 27001:2013/2022, Tecnología de la información. Técnicas de Seguridad (ISO/IEC 27001:2013/2022 – Information technology – Security techniques – Information security management systems – Requirements).

- Resolución 1519 de 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

- Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.

- NTC ISO 27001. Requisitos. Seguridad y Privacidad de la información.

- NTC ISO 27000 Gestión de Riesgos de Seguridad de la Información.

- NTC ISO31000 Gestión del Riesgo.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 del Departamento Administrativo de la Función Pública, de noviembre 2022

- Decreto 767 de 2022, “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”.

6. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La metodología para la identificación, evaluación y gestión de riesgos de los sistemas de gestión vigentes de la SAE se basan en la NTC-ISO 31000, la Guía para la administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP, en su versión 6, Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones y la cual se encuentra definida en PG-GP-001 Política de Gestión de Riesgos y la GM-GP-001 Guía Metodológica de Gestión de Riesgos; estos documentos tienen como objetivo generar un lineamiento para la gestión del riesgo de la SAE que permita la mejora continua y el cumplimiento de los objetivos institucionales mediante el tratamiento de controles, fortaleciendo el desempeño de los procesos y la transparencia en la gestión Institucional.

Por lo anterior y de manera articulada con la Oficina de Integridad, Anticorrupción y Cumplimiento se realiza la gestión de todos los riesgos en la SAE, ya sean operacionales (gestión, fiscales y continuidad de negocio), de integridad (corrupción, conflicto de interés, soborno y fraude) y seguridad de la información. Las actividades de identificación y análisis de los riesgos la realizan con los líderes de cada proceso como propietarios de los activos, por lo cual deben garantizar que los custodios de la información cumplan con los controles establecidos para procurar la confidencialidad, integridad, privacidad y disponibilidad de la información institucional. El objetivo del análisis es identificar los riesgos, evaluar la pertinencia de los controles y determinar el tratamiento del riesgo que lo lleve a un nivel aceptable.

Las estrategias que lograrán la eficacia y eficiencia para la gestión de riesgos en seguridad y privacidad de la información corresponden a:

1. Establecimiento del contexto de riesgos en la Entidad donde se defina los parámetros internos y externos que se deben tomar en consideración para la identificación y valoración del riesgo. Así mismo, se debe tener en cuenta el conocimiento previo de los procesos, proyectos y en general, información de la Entidad.
2. Socializar el proceso de gestión de riesgos en seguridad de la información con la Alta Dirección y líderes de proceso para recibir el apoyo y direccionamiento a las demás partes interesadas (funcionarios, contratistas, proveedores, entre otros).
3. Definir el medio por el cual se realizará las sesiones (virtuales o presenciales) con las partes interesadas (Alta Dirección, Líderes de proceso o a quien se delegue). Esto será sujeto a la disponibilidad del personal y recursos tecnológicos.
4. Revisar y actualizar, si aplica, la herramienta donde se registrará la información de los riesgos en Seguridad de la Información de cada proceso (Matriz de identificación y análisis de riesgos de Seguridad de la Información).
5. Socializar a los involucrados (Alta dirección, líderes de proceso, personal delegado y equipo de Seguridad de la Información) la metodología de gestión de riesgos en Seguridad de la Información, donde se informe el objetivo, alcance, conceptos generales, herramientas y demás información relevante para el entendimiento y agilidad del ejercicio.
6. Ejecución del proceso de gestión de riesgos, es decir la identificación, clasificación, valoración y registro de los riesgos, con la respectiva revisión y aprobación de cada líder de proceso o personal que se designe.
   Nota: Desde la seguridad de la información se brindan los lineamientos, directrices y acompañamiento para la gestión de riesgos en seguridad de la información de los procesos, pero es responsabilidad de cada líder de proceso o a quien se delegue, mantener actualizado la matriz de riesgos a su cargo.
7. Consolidación de la información obtenida durante el ejercicio para un posterior análisis.
8. Elaboración de un informe que contenga de manera ejecutiva los resultados de la identificación, clasificación y valoración de los riesgos en seguridad de la información.
9. Socializar con las partes interesadas (Alta dirección, líderes de proceso, personal delegado y equipo de seguridad de la información) los resultados obtenidos del proceso de gestión de riesgos en seguridad. Durante esta actividad es vital que se mencione la importancia de la gestión de riesgos como un proceso dinámico y que perdure en el tiempo, por tanto, debe ser realizado de manera periódica (al menos una vez al año) por los responsables de los riesgos o cuando se presenten cambios en: la tecnología o los procesos. Por consiguiente, el líder o responsable de los riesgos del proceso debe:

a) Informar cuando se identifique un nuevo riesgo de Seguridad de la Información en el proceso para ser analizado y documentado, en caso de aplicar en la matriz de riesgos.
b) Revisar y actualizar, cuando aplique, la valoración del riesgo (probabilidad e impacto).

6.1 Mapa de Ruta

A continuación, se presentan las actividades que la SAE planea realizar en la vigencia para el tratamiento de riesgos de seguridad de la información:

#	Área que reporta la actividad	Actividad	Fecha inicio	Fecha final	Responsable
1	Oficina de Tecnologías y Sistema de Información	Actualización de Controles Tecnológicos en la Matriz de Riesgos de Seguridad de la Información	01/01/2025	31/12/2025	Jefe(a) de Oficina de Tecnologías y Sistemas de la Información
2	Oficina de Tecnologías y Sistema de Información	Seguimiento Controles Tecnológicos y Materialización de Riesgos	01/04/2025	31/12/2025	Jefe(a) de Oficina de Tecnologías y Sistemas de la Información
3	Oficina de Tecnologías y Sistema de Información	Monitoreo de Riesgos y Vulnerabilidades en la Infraestructura Tecnológica	01/01/2025	31/12/2025	Jefe(a) de Oficina de Tecnologías y Sistemas de la Información
4	Oficina de Tecnologías y Sistema de Información	Monitoreo de Riesgos en Cuentas de Usuarios y Prevención de Ataque	01/01/2025	31/12/2025	Jefe(a) de Oficina de Tecnologías y Sistemas de la Información
5	Oficina de Tecnologías y Sistema de Información	Sensibilización en Seguridad de la Información y Ciberseguridad	01/01/2025	31/12/2025	Jefe(a) de Oficina de Tecnologías y Sistemas de la Información
6	Oficina de Tecnologías y Sistema de Información	Implementación de Microsoft Intune para Administración de Equipos	01/01/2025	31/12/2025	Jefe(a) de Oficina de Tecnologías y Sistemas de la Información

Las copias impresas de este documento no son controladas. Si hace copia impresa verifique su versión en la Oficina Asesora de Planeación.

#	Área que reporta la actividad	Actividad	Fecha inicio	Fecha final	Responsable
7	Oficina de Integridad, Anticorrupción y Cumplimiento	Revisar y/o actualizar de la documentación asociada a riesgos de seguridad de la información	02/05/2025	31/12/2025	Jefe(a) de Oficina de Integridad, Anticorrupción y Cumplimiento
8	Oficina de Integridad, Anticorrupción y Cumplimiento	Socializar la documentación y lineamientos relacionados con la identificación y clasificación de riesgos de seguridad de la Información.	01/07/2025	31/12/2025	Jefe(a) de Oficina de Integridad, Anticorrupción y Cumplimiento
9	Oficina de Integridad, Anticorrupción y Cumplimiento	Identificación de Riesgos de Seguridad de la Información	01/07/2025	31/12/2025	Jefe(a) de Oficina de Integridad, Anticorrupción y Cumplimiento
10	Oficina de Integridad, Anticorrupción y Cumplimiento	Definición de Planes de Tratamiento para la Mitigación de Riesgos de Seguridad de la Información	01/07/2025	31/12/2025	Jefe(a) de Oficina de Integridad, Anticorrupción y Cumplimiento
11	Oficina de Integridad, Anticorrupción y Cumplimiento	Seguimiento a la ejecución de Planes de Tratamiento de Riesgos de Seguridad de la Información	01/07/2025	31/12/2025	Jefe(a) de Oficina de Integridad, Anticorrupción y Cumplimiento