EMPRESAS PUBLICAS DE PIAMONTE A.A.A S.A.S E.S.P.

PIAMONTE CAUCA

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

2025

INTRODUCCIÓN

La Gerencia de Empresas Públicas de Piamonte AAA SAS ESP ha definido un enfoque claro de respaldo y responsabilidad en materia de Seguridad de la Información, considerando este aspecto como una de las dimensiones fundamentales dentro del Modelo Integrado de Planeación y Gestión (MIPG). Para ello, la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) se establece como la herramienta clave que fortalecerá la gestión transversal de la Seguridad de la Información en la SDP, apoyándose en diversos instrumentos que facilitan su implementación.

En este contexto, surge la necesidad de desarrollar un Plan de Tratamiento de Riesgos de Información, el cual permitirá identificar, analizar, evaluar y mitigar los riesgos asociados a la información institucional, tanto en formato físico como digital, en cada uno de los procesos organizacionales. Su propósito es garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad de la información.

OBJETIVO

Elaborar un Plan de Tratamiento de Riesgos de Seguridad de la Información que funcione como una guía metodológica alineada con el instructivo para la Gestión del Riesgo (E-IN-005). Este plan facilitará a los responsables de los procesos de la SDP la adecuada gestión de los riesgos en seguridad y privacidad de la información, centrándose en los activos registrados en el Registro de Activos de Información (RAI). Se priorizarán aquellos activos que, según la evaluación de sus propietarios, presenten un nivel de criticidad alto en cuanto a confidencialidad, integridad y disponibilidad.

ALCANCE

La gestión y tratamiento de riesgos de seguridad de la información se aplicará a todos los activos de información de la SDP identificados en cada proceso y registrados en el RAI. Este proceso se desarrollará conforme a la normativa vigente, siguiendo la metodología establecida por la empresa para la gestión del riesgo y las directrices de la norma ISO 27001. Además, se garantizará su monitoreo, evaluación y mejora continua para asegurar el cumplimiento de los estándares de seguridad.

MARCO NORMATIVO

- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- 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
- CONPES 3854 de 2016: Política Nacional de Seguridad Digital
- Manual para la Implementación de la Política de Gobierno Digital: Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
- Modelo de Seguridad y privacidad de la información – MSPI: Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
- NTC / ISO 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- NTC/ISO 31000:2009: Gestión del Riesgo. Principios y directrices.
- Guía para la administración del riesgo y el diseño de controles en empresaes públicas – Versión 4: Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018.

DEFINICIONES

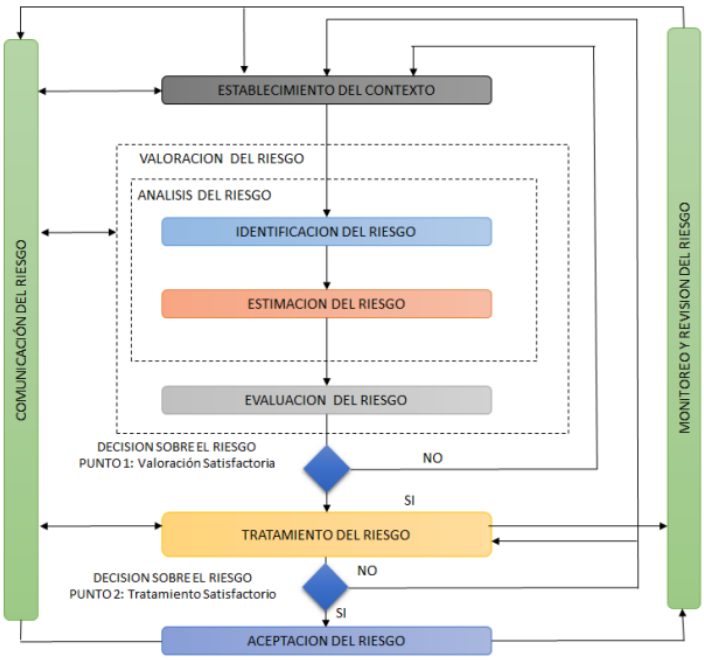
- **Activo:** cualquier elemento que tenga valor para la organización.
- **Análisis del riesgo:** Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa:** Elemento específico que origina el evento.
- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Controles:** Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos:** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo:** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento:** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente:** Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo:** Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **Riesgo aceptable:** Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento.

- **Riesgo:** Posibilidad o probabilidad de que un evento pueda afectar las funciones de la empresa e impactar el logro de sus objetivos.
- **Riesgo de seguridad digital**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Para la gestión de los riesgos de información, se utilizará como referencia el ejercicio documentado de identificación del contexto organizacional, aplicado a los procesos estratégicos, misionales y de apoyo de la empresa. Asimismo, se tomará como base la metodología de tratamiento de riesgos establecida en el Instructivo para la Gestión del Riesgo (E-IN-005). Por ello, este documento se enfocará únicamente en las etapas de identificación y clasificación del riesgo cuando se trate de un "Riesgo de Seguridad Digital".

MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN



El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

1. **Programación y Agendamiento de Entrevistas**: En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la empresa y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

2. **Entrevista con los Líderes:** Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos
3. **Identificación y Calificación de Riesgos:** En esta fase, el líder de proceso evalúa el nivel de impacto vs. probabilidad y los controles existentes para calcular el nivel de riesgo.
   Valoración del Riesgo Residual: En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

INFORMACIÓN DE SEGURIDAD SEGUIMIENTO DE RIESGOS Y REVISIÓN

El seguimiento al tratamiento de riesgos no es solo para velar por el cumplimiento de los controles existentes y los planes de mejora, sino que se debe volver al inicio, es decir, validar si existe un nuevo activo de información y realizar todo el procedimiento del tratamiento de riesgos. Lo mismo sucede con las amenazas, siendo necesario validar periódicamente si existe algún factor interno o externo que impacte los objetivos de la empresa.

También existen escenarios donde se materializan riesgos, para los cuales no se tienen claramente identificados las causas, por lo que, cobra gran importancia el mejoramiento continuo al tratamiento de riesgos y el seguimiento correspondiente.

Otros factores a tener en cuenta corresponden a los criterios utilizados para medir el riesgo, ya que pueden existir nuevas reglamentaciones que cambien la clasificación de un activo o la criticidad de este.

Dentro de estos factores se tiene:

- Contexto legal y ambiental
- Contexto de competencia en el mercado
- Categorías y valor de los activos
- Criterios de impacto
- Criterios de evaluación del riesgo
- Criterios de aceptación del riesgo
- Costo total de la propiedad
- Recursos necesarios
- Enfoque para la valoración del riesgo

PLAN DE MEJORAMIENTO CONTINUO

A continuación, se detallan las actividades que se desarrollarán para fortalecer el tratamiento de riesgos de seguridad digital para los activos de información de la empresa.

IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS

Identificar los riesgos de seguridad digital basados y realizar los acompañamientos que se requieran a los funcionarios, teniendo en cuenta que cada área tiene el conocimiento claro y preciso de su proceso y pueden identificar la forma en que la confidencialidad, integridad y disponibilidad, se pueden ver afectadas.

RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información identificados en la empresa, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

- Los líderes de las áreas solicitarán a la gerencia la inclusión de los riesgos en el mapa de riesgos institucional, instrumento en donde se registran los riesgos identificados, su valoración y sus controles, para su seguimiento y control.
- La oficina de control interno apoyará a los responsables de las áreas en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo No aceptable.

Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.

YON FREDY CUELLAR LOPEZ
Gerente Empresas Públicas de Piamonte AAA S.A.S. E.S.P

Proyectó/Aprobó: Ing. Yon Fredy Cuellar López – Gerente Empresas Públicas de Piamonte AAA S.A.S. E.S.P.