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

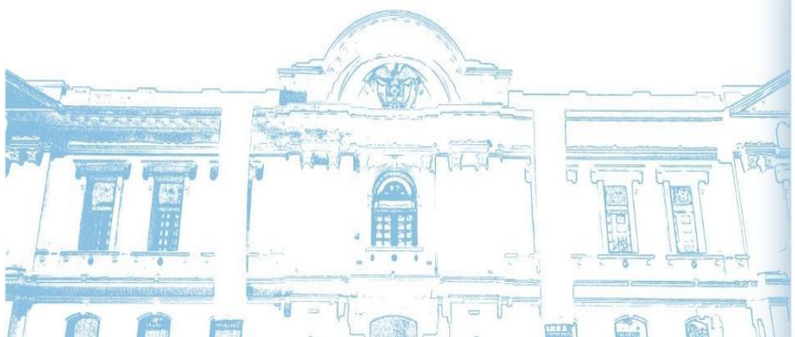

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La seguridad y privacidad de la información son esenciales para proteger la integridad, confidencialidad y disponibilidad de los datos manejados por la alcaldía.

Este plan de tratamiento de riesgos se centra en identificar, analizar, evaluar, y mitigar los riesgos asociados con la seguridad y privacidad de la información. Al implementar este plan, la alcaldía distrital de santa marta busca asegurar que sus sistemas y datos sean resistentes a amenazas internas y externas, y que cumplan con las normativas legales y mejores prácticas internacionales.

2. OBJETIVO

El objetivo de este plan es establecer un marco integral para la gestión de riesgos de seguridad y privacidad de la información, garantizando la protección continua de los datos sensibles manejados. Este marco busca:

- Identificar y evaluar los riesgos asociados a la seguridad y privacidad de la información.
- Implementar controles y medidas efectivas para mitigar dichos riesgos.
- Promover una cultura organizacional de conciencia y responsabilidad en la protección de la información.
- Cumplir con las leyes y regulaciones aplicables en materia de seguridad y privacidad de la información.
- Mejorar continuamente los procesos y procedimientos relacionados con la seguridad de la información.

3. ALCANCE

Este plan de tratamiento de riesgos de seguridad y privacidad de la información se aplica a todos los procesos, sistemas, activos de información y personal de la alcaldía distrital de santa marta, incluyendo:

- Todos los datos y sistemas de información gestionados por la alcaldía.
- Todos los directivos, funcionarios y terceros que trabajan o colaboran con la alcaldía.
- Todas las ubicaciones físicas y virtuales donde se almacena procesan o transmite información.
- Todas las actividades relacionadas con la gestión de la información, desde su creación y almacenamiento hasta su eliminación o archivado.
- Las relaciones con terceros que impliquen el manejo de información, asegurando que estos también cumplan con los estándares de seguridad y privacidad establecidos por la alcaldía.

Este alcance amplio asegura que todos los aspectos relevantes de la gestión de la información estén cubiertos, permitiendo una protección robusta y holística de los datos en toda la entidad.

4. TÉRMINOS Y DEFINICIONES

Activos: cualquier cosa que tenga valor para la entidad es considerada un activo en este caso la información es un activo.

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Alcaldía Distrital de Santa Marta y, en consecuencia, debe ser protegido.

Amenaza: causa potencial de un incidente no deseado, que puede producir un daño a un sistema

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados; se encuentra resguardada o salvaguardada en nuestros centros de datos con control de acceso a los usuarios a cada información.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerar, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

MINTIC: Ministerio de Tecnología de la Información y las Comunicaciones.

MOP: Modelo de operación por procesos.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Política: su objetivo es establecer, a partir de la observación de hechos de la realidad política, principios generales acerca de su funcionamiento.

Riesgo: riesgo es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Seguridad de la Información: se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la Información SGSI: Es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Alcaldía Distrital de Santa Marta, o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

TI: Tecnología de información.

TIC: Tecnologías de la información y la comunicación.

Terceros: persona o entidad que se reconoce como independiente.

Usuario: Es aquella persona que usa una cosa o servicio habitualmente. Un usuario es un conjunto de permisos y de recursos a los cuales se tiene acceso.

5. RESPONSABLES

Los directivos, funcionarios y terceros que laboren o tengan relación con la Alcaldía Distrital de Santa Marta, con el acompañamiento de la Dirección de TIC.

6. MARCO NORMATIVO

- Constitución Política de Colombia: Artículo 15: Derecho a la intimidad y protección de datos personales.
- MINTIC: Seguridad y Privacidad de la Información - Guía No. 2
- MIPG: Modelo Integrado de Planeación y Gestión
- Ley 1581 de 2012 (Ley de Protección de Datos Personales): Regula la protección de datos personales y establece las obligaciones para las entidades que manejan información personal.
- Decreto 1377 de 2013: Reglamenta la Ley 1581 de 2012, estableciendo disposiciones para la protección de datos personales.
- Ley 1273 de 2009 (Delitos Informáticos) Tipifica los delitos informáticos y establece las sanciones correspondientes.
- Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública) Garantiza el derecho de acceso a la información pública y establece las responsabilidades de las entidades públicas en la gestión de la información.
- Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC): Incluye normas relacionadas con la seguridad de la información en el sector de tecnologías de la información y comunicaciones.
- Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

- 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”.

- Resolución 00500 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”.

- Circular Única de la Superintendencia de Industria y Comercio (SIC): Establece directrices y recomendaciones para el cumplimiento de la normativa de protección de datos personales.

- Directrices y Políticas Internas de la Alcaldía Distrital de Santa Marta

- Políticas y procedimientos internos desarrollados por la alcaldía para la gestión de la seguridad y privacidad de la información, alineados con el marco normativo externo.

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

La preservación de la información surge como una prioridad ineludible para la Alcaldía y la Dirección de TIC está comprometida en impulsar los principios fundamentales de confidencialidad, disponibilidad e integridad sobre todos los activos de información que gestiona. En este contexto, el año 2024 se distingue como un momento trascendental en el fortalecimiento de la seguridad y privacidad de la información en el Distrito de Santa Marta. Esto se logra a través del desarrollo e implementación del Plan de Seguridad y Privacidad de la Información y tratamiento de riesgos de seguridad y privacidad de la información, donde la participación de todas las dependencias a nivel central del Distrito representa un avance significativo. Esta colaboración ha permitido ampliar el alcance y mejorar la visibilidad de los activos de información que están bajo su responsabilidad.

Al analizar las modalidades de ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información en la vigencia 2024, se distinguieron dos enfoques principales: por dependencia o de forma individual. En la modalidad por dependencia, se orienta la ejecución de manera centralizada, integrando todas las Secretarías, Direcciones, y demás Dependencias en un solo plan. Por otro lado, en la modalidad individual, se aborda la ejecución del plan de forma específica por cada Secretaría, subdirección, unidad y equipo que conforma la dependencia.

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información a cargo del Distrito de Santa Marta, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados.

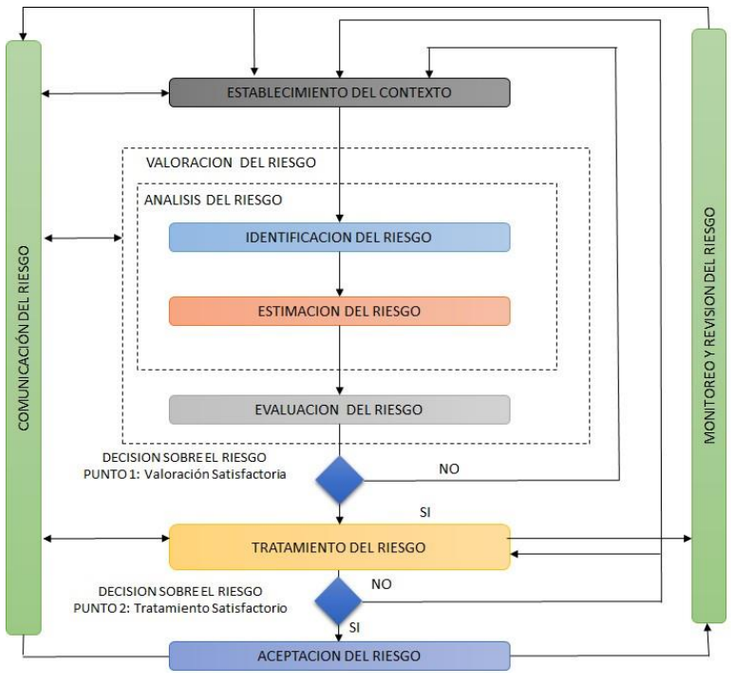

Ilustración 1. Proceso para la Administración del Riesgo

Este conjunto de normas ISO /IEC promueve la adopción del enfoque basado en procesos, para que una organización funcione eficazmente, se debe identificar y gestionar muchas actividades, por lo que se considera como proceso a cualquier actividad que consume recursos y que, además, su gestión promueva la transformación de entradas en salidas. El enfoque basado en procesos consiste en que la organización identifique las actividades del funcionamiento de esta y la interacción entre las actividades; así, para la gestión de la Seguridad de la Información se hace énfasis en la importancia de la norma ISO 27001:2013.

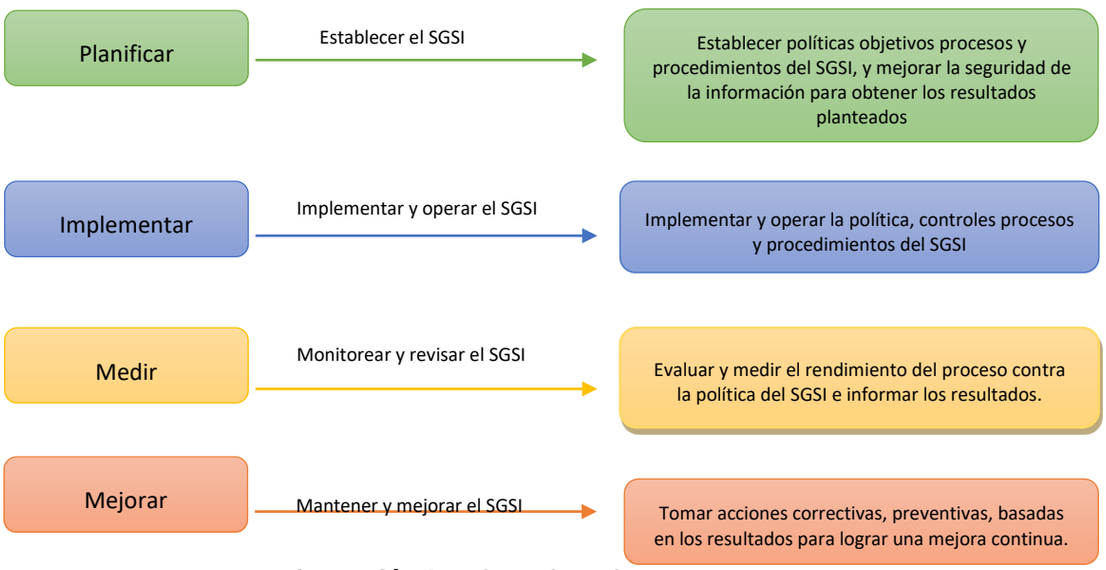

Ilustración 2. enfoque basado en procesos

8. CRITERIOS DE EVALUACIÓN DE RIESGOS DE SEGURIDAD

La evaluación de riesgos de seguridad de la información es un proceso crítico para identificar, analizar y gestionar los riesgos que pueden afectar a la alcaldía distrital de santa marta. A continuación, se describen los criterios principales que se consideran para la evaluación de estos riesgos:

- **Impacto:** Consecuencias potenciales que un riesgo puede tener sobre la organización.

- **Probabilidad de ocurrencia:** La probabilidad de ocurrencia mide la posibilidad de que un riesgo se materialice.

VALOR DE IMPACTO			
	NIVEL	**DESCRIPCION**	**ESCALA**
1	**Insignificante**	Impacta negativamente de forma leve la imagen y operación de un rol. No tiene impacto Financiero para la Entidad o sus procesos. Impacta negativamente, posibilidad de recibir multas.	**>=1 y <=4**
2	**Menor**	Impacta negativamente la imagen y de manera importante la operación de un proceso. Se pueden presentar sobrecostos debido a reprocesos a nivel de un proceso. Impacta negativamente, posibilidad de recibir multas.	**>=5 y <=8**
3	**Moderado**	Afecta negativamente la imagen Institucional a nivel regional por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos. Se pueden presentar sobrecostos por reprocesos y aumento de carga operativa, no sólo en el proceso evaluado sino a otros procesos. Impacta negativamente, posibilidad de recibir una investigación disciplinaria.	**>=9 y <=12**
4	**Mayor**	Imagen Institucional a nivel nacional afectada, al igual que la operación por el incumplimiento en la prestación de servicios de la Entidad o el cumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos por reprocesos significativos para una sede seccional de la Institución. Impacta negativamente, posibilidad de recibir una investigación fiscal.	**>=13 y <=16**
5	**Catastrófico**	Imagen Institucional afectada a nivel nacional e Internacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la Institución y el incumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos debido a reprocesos y aumento de carga operativa importante en toda la Entidad. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	**>=17 y <= 20**

- **Vulnerabilidad:** La vulnerabilidad se refiere a la debilidad o deficiencia en los controles de seguridad que podría ser explotada por una amenaza.

ESCALA DE PROBABILIDAD		
NIVEL		**DESCRIPCION**
1	**Raro**	Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre.
2	**Improbable**	Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	**Posible**	Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre.
4	**Probable**	Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5	**Casi Seguro**	Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

- **Amenaza:** La amenaza es cualquier circunstancia o evento con el potencial de causar daño a los activos de información.

ZONA DE RIESGO
B: Zona de riesgo baja (color verde) 5 zonas siendo la Z-5 la de mayor riesgo
M: Zona de riesgo moderada (color amarillo) 4 zonas siendo la Z-9 la de mayor riesgo
A: Zona de riesgo alta (color rojo) 8 zonas siendo la Z-17 la de mayor riesgo

E: Zona de riesgo extrema (color vino tinto) 8 zonas siendo la Z-25 la de más alto riesgo

Fuente: imagen tomada del plan de tratamientos de riesgos de seguridad y privacidad de la información: indercultura putumayo.

- **Consecuencias:** Las consecuencias de un riesgo se refieren a los efectos que puede tener sobre la organización:

- **Controles:** Los controles existentes son las medidas de seguridad que ya están implementadas para mitigar riesgos.

9. VALORACION DEL RIESGOS

La valoración del riesgo es un proceso integral que combina la evaluación del impacto, la probabilidad de ocurrencia, la vulnerabilidad, y los controles existentes para determinar la criticidad de cada riesgo y su prioridad de tratamiento. A continuación, se describe cómo se llevará a cabo la valoración del riesgo en la alcaldía distrital de santa marta:

a) **Riesgo: Pérdida de datos por ataque de ransomware**
   - Impacto: Alto
   - Probabilidad: Media
   - Vulnerabilidad: Alta (debido a falta de copias de seguridad adecuadas)
   - Controles Existentes: Antivirus instalado, pero no actualizado regularmente
   - Valoración del Riesgo: Riesgo Alto

b) **Riesgo: Acceso no autorizado a datos sensibles por parte de empleados**
   - Impacto: Medio
   - Probabilidad: Alta
   - Vulnerabilidad: Media (controles de acceso, pero falta de supervisión)
   - Controles Existentes: Políticas de acceso a datos, pero sin monitoreo constante
   - Valoración del Riesgo: Riesgo Alto

c) **Riesgo: Interrupción de servicios por fallo de hardware**
   - Impacto: Medio
   - Probabilidad: Baja
   - Vulnerabilidad: Baja (hardware con mantenimiento regular)
   - Controles Existentes: Plan de contingencia y respaldo de hardware
   - Valoración del Riesgo: Riesgo Bajo

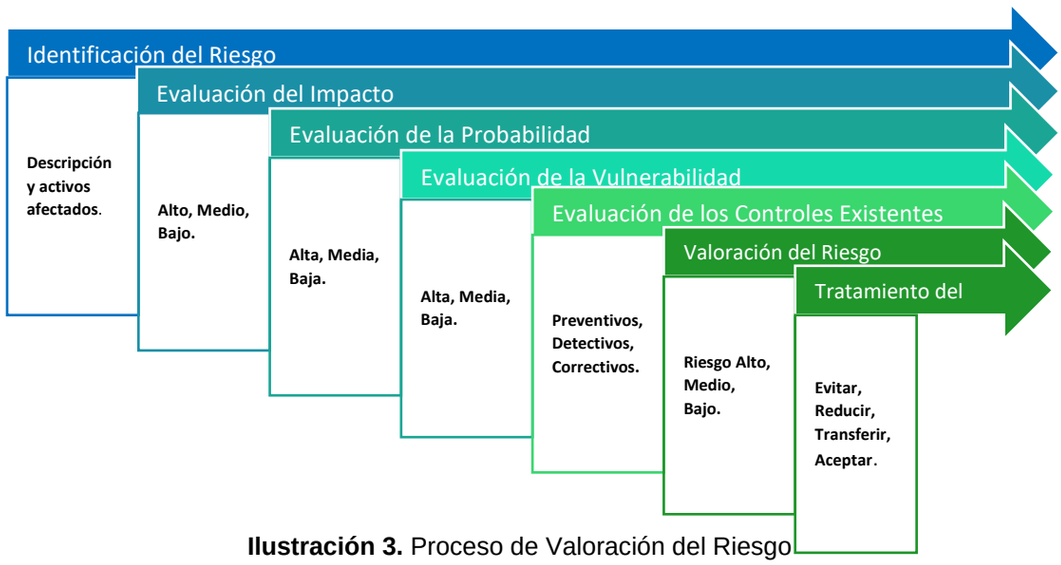

Ilustración 3. Proceso de Valoración del Riesgo

10. TRATAMIENTO DEL RIESGO

Una vez realizada la valoración, se procede al tratamiento del riesgo:

- Modificar los planes para eliminar el riesgo.
- Implementar controles adicionales para reducir la probabilidad o impacto.
- Externalizar o asegurar el riesgo.
- Decidir no tomar ninguna acción adicional si el riesgo es aceptable.

11. IDENTIFICACIÓN DEL RIESGO

La identificación de los riesgos es el primer y fundamental paso en el proceso de gestión de riesgos. Este proceso implica descubrir y describir los riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información en la alcaldía distrital de santa marta. A continuación, se detallan los métodos utilizados para identificar los riesgos:

- Definición del Contexto
- Identificación de Activos
- Identificación de Amenazas
- Identificación de Vulnerabilidades
- Métodos de Identificación de Riesgos
- Registro de Riesgos

12. ESTIMACIÓN DEL RIESGO

La estimación del riesgo busca cuantificar o calificar los riesgos identificados en términos de su impacto y probabilidad de ocurrencia. Este proceso permite priorizar los riesgos y determinar las acciones necesarias para su gestión. A continuación, se detallan los métodos para la estimación del riesgo:

- **Identificación del Riesgo:** Se define claramente el riesgo, incluyendo la amenaza y la vulnerabilidad asociada.
- **Determinación del Impacto:** El impacto de un riesgo es la consecuencia que puede tener sobre la entidad. Se consideran diferentes dimensiones de impacto:
- **Determinación de la Probabilidad:** La probabilidad de ocurrencia de un riesgo mide la frecuencia con la que puede materializarse.

13. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD

El tratamiento de los riesgos de seguridad implica desarrollar e implementar estrategias para gestionar y mitigar los riesgos identificados. Este proceso asegura que los riesgos sean abordados de manera efectiva para proteger la confidencialidad, integridad y disponibilidad de la información en la alcaldía distrital de santa marta. A continuación, se detallan los métodos para el tratamiento de los riesgos de seguridad:

- Identificación de Opciones de Tratamiento
- Selección de Estrategias de Tratamiento
- Desarrollo de Planes de Tratamiento
- Implementación de Medidas de Control

14. ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS DE LA ALCALDÍA DISTRITAL

El plan de tratamiento de riesgos de la alcaldía distrital de santa marta incluye una serie de actividades organizadas en diferentes etapas para garantizar la identificación,

evaluación, mitigación y monitoreo de los riesgos de seguridad de la información. A continuación, se describen las actividades clave a desarrollarse en cada etapa del plan:

a) Identificación de Riesgos

- **Inventario de Activos:** Crear y mantener un inventario actualizado de todos los activos de información, incluyendo hardware, software, redes, personal, sitios y estructuras organizativas.
- **Clasificación de Activos**: Clasificar los activos en primarios y de soporte, según su importancia y función en la organización.
- **Identificación de Amenazas:** Identificar amenazas potenciales que pueden afectar a los activos de información, mediante entrevistas, inspecciones físicas y el uso de herramientas de escaneo automatizado.
- **Identificación de Vulnerabilidades:** Identificar las vulnerabilidades que podrían ser explotadas por las amenazas, evaluando las debilidades en los controles actuales.

b) Evaluación y Valoración de Riesgos

- **Análisis de Impacto:** Evaluar el impacto potencial de cada amenaza sobre los activos de información, considerando la confidencialidad, integridad y disponibilidad.
- **Probabilidad de Ocurrencia:** Estimar la probabilidad de ocurrencia de cada amenaza, basada en la frecuencia histórica y las condiciones actuales.
- **Cálculo del Nivel de Riesgo:** Calcular el nivel de riesgo combinando la probabilidad y el impacto, utilizando matrices de riesgo o metodologías similares.
- **Priorización de Riesgos:** Priorizar los riesgos identificados según su nivel de riesgo para determinar cuáles requieren una atención más urgente.

IMPACTO	VALOR	EVALUACION				
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	PROBABILI DAD	Raro	Improbable	Posible	Probabl e	Casi Seguro

Matriz IP evaluación del riesgo

c) Desarrollo de Estrategias de Tratamiento

- **Definición de Opciones de Tratamiento:** Identificar y evaluar las opciones de tratamiento de riesgos, incluyendo evitar, reducir, compartir o aceptar el riesgo
- **Selección de Estrategias:** Seleccionar las estrategias de tratamiento más apropiadas para cada riesgo, considerando el costo-beneficio, viabilidad técnica y cumplimiento normativo.
- **Desarrollo de Planes de Acción:** Elaborar planes de acción detallados para implementar las estrategias seleccionadas, incluyendo las medidas específicas, responsables, recursos necesarios y cronograma.

d) Implementación de Medidas de Control

- **Controles Administrativos:** Implementar políticas, procedimientos, estándares y directrices para gestionar los riesgos de seguridad de la información.
- **Controles Técnicos:** Desplegar soluciones tecnológicas como firewalls, sistemas de detección de intrusos, cifrado, etc.
- **Controles Físicos:** Establecer medidas de seguridad física, como controles de acceso, vigilancia y protección de sitios.
- **Controles Humanos:** Capacitar al personal en prácticas de seguridad, asignar roles y responsabilidades claras, y fomentar una cultura de seguridad.

15. MONITOREO Y REVISIÓN

El monitoreo y revisión constante de las medidas de control de seguridad son esenciales para asegurar su efectividad y adecuación en el tiempo. A continuación, se describe cómo se llevarían a cabo estas actividades:

a) Auditorías y Evaluaciones Regulares

Auditorías Internas: Se realizarán auditorías internas para evaluar el cumplimiento de las políticas de seguridad y la efectividad de los controles implementados. Estas auditorías pueden incluir revisiones de acceso a sistemas, evaluaciones de configuración de seguridad y revisiones de registros de actividades.

Auditorías Externas: Contratar auditores externos para realizar evaluaciones independientes de los controles de seguridad, proporcionando una visión imparcial y asegurando que se cumplan las normas y regulaciones aplicables.

Evaluaciones de Riesgos: Realizar evaluaciones de riesgos regulares para identificar nuevos riesgos y re-evaluar los riesgos existentes, asegurando que se mantengan actualizados los planes de tratamiento de riesgos.

b) Monitoreo Continuo

Sistemas de Detección de Intrusos (IDS/IPS): Implementar y monitorear sistemas de detección y prevención de intrusos para identificar y responder rápidamente a posibles incidentes de seguridad.

Monitoreo de Red: Utilizar herramientas de monitoreo de red para detectar actividades sospechosas, anomalías en el tráfico y posibles brechas de seguridad.

Monitoreo de Logs: Revisar y analizar registros de actividades de sistemas, aplicaciones y dispositivos para identificar eventos inusuales o indicios de compromisos de seguridad.

c) Revisión de Políticas y Procedimientos

Actualización de Políticas: Revisar y actualizar periódicamente las políticas de seguridad de la información para reflejar cambios en el entorno de riesgos, tecnologías y regulaciones.

Revisión de Procedimientos: Evaluar y mejorar continuamente los procedimientos operativos de seguridad para asegurar su efectividad y adecuación a las necesidades de la organización.

d) Informe de Incidentes

Registro de Incidentes: Documentar todos los incidentes de seguridad, detallando la naturaleza del incidente, las acciones tomadas, y las lecciones aprendidas.

Análisis de Incidentes: Realizar análisis post-incidente para identificar causas raíz, evaluar la efectividad de la respuesta y desarrollar planes de mejora para prevenir futuros incidentes.
Comunicación: Informar a las partes interesadas relevantes sobre los incidentes de seguridad y las medidas correctivas implementadas.

16. MEJORA CONTINUA

La mejora continua en la gestión de riesgos de seguridad de la información es fundamental para adaptarse a nuevas amenazas y mejorar la resiliencia de la organización. Aquí se describen las actividades para lograr una mejora continua:

a) Ciclo de Mejora Continua (PDCA)

Planificar (Plan): Identificar áreas de mejora, establecer objetivos y metas, y desarrollar planes de acción basados en los resultados del monitoreo y revisión.

Hacer (Do): Implementar las acciones planificadas y ejecutar las mejoras necesarias en los controles de seguridad.

Verificar (Check): Evaluar la efectividad de las acciones implementadas, revisar los resultados y comparar con los objetivos establecidos.

Actuar (Act): Tomar medidas correctivas y ajustar los planes de acción para abordar cualquier desviación o área que necesite mejora.

b) Capacitación y Concienciación

Programas de Capacitación: Desarrollar y ejecutar programas de capacitación continuos para el personal sobre las políticas de seguridad, buenas prácticas y nuevas amenazas emergentes.

Campañas de Concienciación: Realizar campañas de concienciación regulares para mantener al personal informado y vigilante sobre los riesgos de seguridad de la información.

c) Análisis de Tendencias y Nuevas Amenazas

Vigilancia de Amenazas: Mantenerse informado sobre las tendencias emergentes en ciberseguridad, nuevas amenazas y vulnerabilidades que puedan afectar a la organización.

Evaluaciones de Tecnología: Revisar y evaluar nuevas tecnologías y soluciones de seguridad que puedan mejorar la protección de los activos de información.

d) Retroalimentación y Mejora de Procesos

Encuestas y Feedback: Recopilar retroalimentación del personal y de las partes interesadas sobre la efectividad de las políticas y controles de seguridad.

Análisis de Procesos: Revisar y mejorar los procesos de gestión de riesgos, asegurando que sean eficientes y eficaces en la mitigación de riesgos.

e) Revisión de Controles y Estrategias

Evaluación de Controles: Revisar periódicamente la efectividad de los controles de seguridad implementados y realizar ajustes según sea necesario.
Actualización de Estrategias: Revisar y actualizar las estrategias de tratamiento de riesgos para asegurarse de que sigan siendo relevantes y efectivas en el contexto actual de la organización.

17. Plan de Trabajo para el Tratamiento de Riesgos de Seguridad de la Información

Actividad	Responsable	2 semestre 2024					
		J	A	S	O	N	D
Realizar la identificación, clasificación, tratamiento y divulgación de Incidentes seguridad de la información materializados en atención a los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las Secretarías, Direcciones, Gerencias, jefaturas y demás dependencias nivel central del Distrito, encabezado por la Dirección de TIC.	X	X	X	X	X	
Realizar la identificación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las Secretarías, Direcciones, Gerencias, jefaturas y demás dependencias nivel central del Distrito encabezado por la Dirección de TIC.		X	X	X	X	X
Realizar la adquisición e implementación de controles de seguridad de la información identificados, para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las Secretarías, Direcciones, Gerencias, jefaturas y demás dependencias nivel central del Distrito encabezado por la Dirección de TIC.		X	X	X	X	X
Realizar el seguimiento a las actividades de identificación, adquisición e implementación de controles de seguridad de la información, así como de tratamiento de incidentes de seguridad de la información, para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las Secretarías, Direcciones, Gerencias, jefaturas y demás dependencias nivel central del Distrito encabezado por la Dirección de TIC.			X	X	X	X

18. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS	
Versión	**Descripción de la modificación**
1	Creación del documento
2	Ajustes año 2024 acuerdo con la articulación MIPG y normas de MINTC

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jhon Fredy Velásquez **Cargo:** Profesional Especializado **Fecha:** 31-may-2024 **Firma:**	**Nombre: Rigoberto García Guillot** **Cargo:** Director TIC **Fecha:** 10-jun-2024 **Firma:** **Nombre: Jackelin Alejandra Granados** **Cargo:** Técnico administrativo - SIG **Fecha:** 02-jun-2024 **Firma:**	**COMITÉ GESTION DE DESEMPEÑO**