1. OBJETIVO

Mitigar los Riesgos de Seguridad y Privacidad de la información (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos, Perdida de Disponibilidad de los activos) identificados en el IMETY que impidan el logro de los objetivos estratégicos y del proceso mediante acciones priorizadas con un enfoque preventivo que generen una mayor confianza en la información que se almacena y maneja en la Entidad.

2. ALCANCE

Este Modelo es aplicable a cualquier sistema de información o aspecto particular de control del IMETY, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información.

3. DEFINICIONES

- **Activo:** Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección.
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Información:** Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un

conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.
- **Información pública reservada:** Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **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 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.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos. • Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

4. CONDICIONES GENERALES

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5. DESARROLLO DEL DOCUMENTO

VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

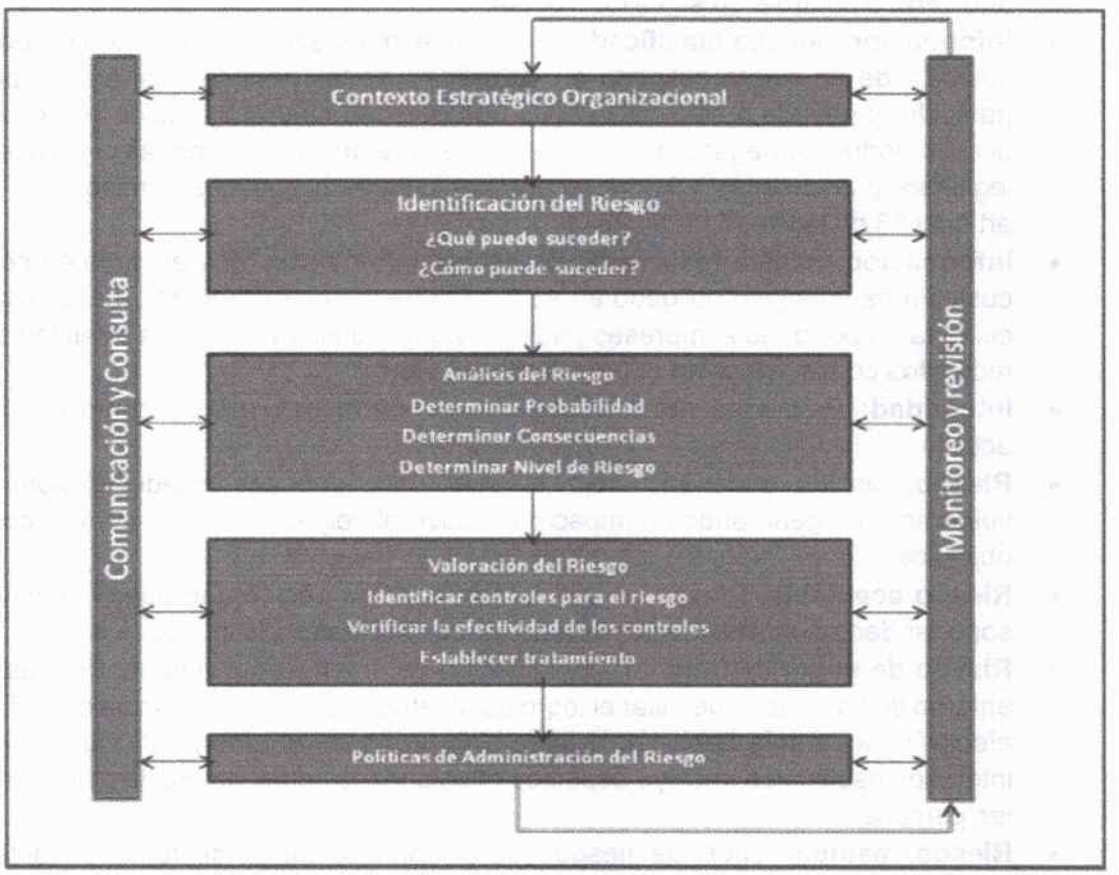


Imagen Tomada de la Cartilla de Administración de Riesgos del DAFP

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

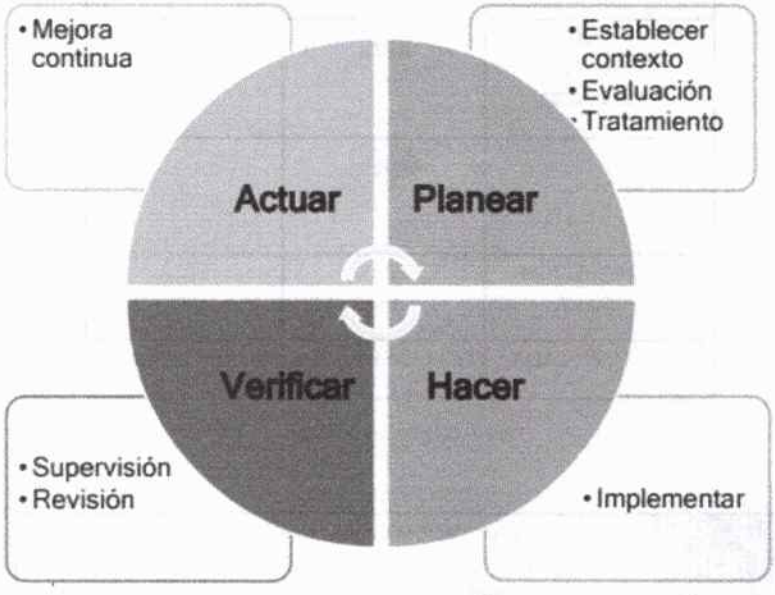
Tabla 2. Niveles de Clasificación

Fuente: Guía No.07 de Gestión del Riesgo MInTic

5.1. IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto el IMETY. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4, emitida por el Departamento Administrativo de la Función Pública.

La gestión de riesgos de seguridad de la información se puede enmarcar dentro del ciclo PHVA tal como se muestra en la siguiente ilustración (ISO 27001:2013):



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

ACTIVIDAD	DESCRIPCIÓN	FECHA TENTATIVA
Programación y Agendamiento de Entrevistas	En esta fase se seleccionan los procesos incluidos en el alcance del SG del IMETY y se procede a programar y a agendar a los líderes de los procesos, para la identificación de riesgos.	Febrero 2023
Entrevista con los Líderes	Se entrevista a cada líder de proceso, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información adoptados por el IMETY, los cuales se consignan en la Matriz de Riesgos.	Febrero y Marzo 2023
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.	Febrero y Marzo 2023
Valoración del Riesgo Residual	En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.	Febrero y Marzo 2023

5.2 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar acciones para

los riesgos ubicados en escala de alto y extremo, cada líder responsable de los riesgos identificados con el apoyo de Gestión de Planeación y Gestión TICS, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del tratamiento de riesgos de la matriz de riesgos en donde se definen las opciones de tratamiento, acciones para mitigar, responsable de las acciones y tiempo para su implementación.

Los riesgos ubicados en la escala de bajo y moderado, se consideran un riesgo aceptable por lo tanto no se definirán acciones para mitigar estos riesgos.

El proceso de tratamiento de los riesgos de seguridad de la información está compuesto por las siguientes actividades:

ACTIVIDAD	DESCRIPCIÓN	FECHA TENTATIVA
Revisión, ajustes, al plan de tratamiento de los riesgos	En esta fase se seleccionan los riesgos ubicados en la escala de extremo y alto en el IMETY y se procede a definir las opciones de tratamiento, acciones para mitigar, responsable de las acciones y tiempo para su implementación.	Febrero de 2023, inicial y una fecha final al

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o acepta**r el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

5.3. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Cuatrimestralmente el líder de cada proceso deberá realizar el seguimiento a la implementación de las acciones establecidas para mitigar los riesgos, determinando su

estado y nivel de implementación, asimismo identificar si se efectúo materialización del riesgo, esta información quedará consignada en la Matriz de Riegos.

ACTIVIDAD	DESCRIPCIÓN	FECHA TENTATIVA
Monitoreo y Seguimiento	En esta fase se determina el estado de las acciones del tratamiento de los riesgos y nivel de implementación, así mismo identificar si se efectúo materialización del riesgo.	Abril, Julio, Octubre y Diciembre de 2023

5.4. OPORTUNIDAD DE MEJORA

IMETY no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

6. RECURSOS

IMETY, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos.

Recurso Humano: El proceso de Gestión de Tecnologías de la Información y Comunicación a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información. La aplicación de la metodología y seguimiento a la administración de riesgos de seguridad y privacidad de la información se realizará por parte del Proceso de Gestión de Planeación conjuntamente con los riesgos de gestión y riesgos de corrupción. Todas las actividades se realizan articuladas con los líderes de procesos y el Comité Institucional de Gestión y Desempeño integrando así un grupo multidisciplinario que contribuye al mejoramiento continuo.

Recursos Técnicos: Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital – Versión 5 - Diciembre de 2020 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI) y Guía No.07 de Gestión del Riesgo Min TIC

Recursos Financieros: Para la adquisición de elementos, equipos y entre otros que contribuyan al cumplimiento de las acciones establecidas para la mitigación de los riesgos.

7. INDICADORES

La medición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizará 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.

REVISO: RUBEN DARIO BARRETO	**CARGO:** CONTRATISTA TIC	**FIRMA:**
APROBO: RUBEN DARIO MILLAN	**CARGO:** DIRECTOR	**FIRMA:**

ANEXOS

Anexo A. Control de Cambios

Versión	Fecha (dd/mm/aaaa)	Revisado por:	Aprobado por:	Descripción de la actualización
01	17/01/2019	Manuel Alberto Torres	Carlos Arturo Tello Becerra	Creación del Plan
02	28/06/2019	Christian Valencia	Carlos Arturo Tello Becerra	Modificación del plan se incluye definiciones y metodología
03	30/01/2020	Ruben Barreto/ Johana Orejuela	Jaime Sánchez Lenis	Se actualiza del objetivo riesgos de la metodología, matriz de calificación se incluye presupuesto y medición del modelo
04	27/01/2021	Jhon Jairo Ortiz	Jaime Sánchez Lenis	Modificación del objetivo del plan, inclusión de definiciones, condiciones generales, clasificación de los activos de información, oportunidades de mejora, recursos e indicadores.
05	23/09/2021	Ruben Barreto	Jaime Sánchez Lenis	Modificación del plan la periodicidad para realizar seguimiento será cuatrimestral.
06	24/01/2022	Claudia Vélez Arias	Jaime Sánchez Lenis	Modificacion

06	30/01/2023	Ruben Dario Barreto	Ruben Dario Millan	Se usa nueva guía de la función pública y se cambian fechas para la administración de los riesgos y establecer controles en el año 2023.