Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Tabla de contenido

1. DERECHOS DE AUTOR

Metrolínea S.A. para la elaboración del documento acoge como referencia la Guía para la Gestión de riesgos del Ministerio de Tecnologías de la Información y las Comunicaciones e igualmente toma como referencia el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información elaborado por la alcaldía mayor de Bogotá en el año 2021 con la finalidad de aportar al componente de seguridad y privacidad de la información, adaptándolo a las situaciones fácticas particulares y necesidades de la entidad.

2. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

3. OBJETIVO

Establecer lineamientos para que Metrolínea S.A. a través de mejores prácticas de seguridad y privacidad de la información, se fortalezca y adopte medidas y acciones encaminadas a modificar, reducir o eliminar riesgos relacionados que atenten contra la seguridad y tratamiento de la información de la Entidad.

4. ALCANCE

Inicia con la detección del evento de riesgo y su tratamiento final, en cualquier área de a la entidad e involucra a todos los servidores públicos, contratistas y/o terceros.

5. GLOSARIO

- **Ataque:**
  Cualquier acción deliberada con el objetivo de violar los mecanismos de seguridad de un sistema de información.

- **Auditoria de Seguridad:**
  Estudio y examen independiente de registros históricos y actividades de un sistema de información con el objetivo de comprobar la solidez de los controles del sistema, alinear los controles con la estructura de seguridad y procedimientos operativos establecidos a fin de detectar brechas en la seguridad y recomendar modificaciones en los procedimientos, controles y estructuras de seguridad.

- **Autenticidad:**

Aseguramiento de la identidad u origen.

- **Certificación:**
  Confirmación del resultado de una evaluación y de que los criterios de la evaluación utilizados fueron correctamente aplicados.

- **Confidencialidad:**
  Aseguramiento de que la información es accesible sólo por aquellos autorizados a tener acceso.

- **Degradación:**
  Pérdida de valor de un activo como consecuencia de la materialización de una amenaza

- **Disponibilidad:**
  Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a sus activos asociados.

- **Estado de riesgo:**
  Caracterización de activos por riesgo residual. "Lo que puede pasar tomando en consideración que las salvaguardas han sido desplegadas".

- **Evento de seguridad:**
  Momento en que la amenaza existe y pone en riesgo activos, procedimientos o información.

- **Evaluación de Medidas de Seguridad:**
  Evaluación de las medidas de seguridad existentes con relación al riesgo que enfrentan.

- **Frecuencia:**
  Tasa de ocurrencia de una amenaza

- **Gestión de riesgos:**
  Selección de implementación de medidas de seguridad para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. La gestión de riesgos se basa en resultados obtenidos en el análisis de riesgos.

- **Impacto:**
  Consecuencia que sobre un activo tiene la materialización de una amenaza.

- **Impacto residual:**
  Impacto remanente en el sistema tras la implantación de las medidas de seguridad determinadas en el plan de seguridad de la información.

- **Inside:**
  Empleado desleal quien, por motivos de desinterés, falta de capacidad intelectual y/o

analítica, problemas psicológicos o psiquiátricos, corrupción, colusión u otros provoca daños en forma deliberada en la empresa en que trabaja, incumpliendo conscientemente con normas y procedimientos establecidos, robando o hurtando activos (físicos o información) con objetivos económicos o simplemente de daño deliberado.

- **Integridad**
  Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

- **Matriz de riesgos**
  Relación de las amenazas y vulnerabilidades a que están expuestos los activos de información.

- **Plan de seguridad**
  Conjunto de tareas orientadas a afrontar el riesgo del sistema.

- **Riesgo:**
  Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños y / o perjuicios a la Organización.

- **Seguridad:**
  Capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

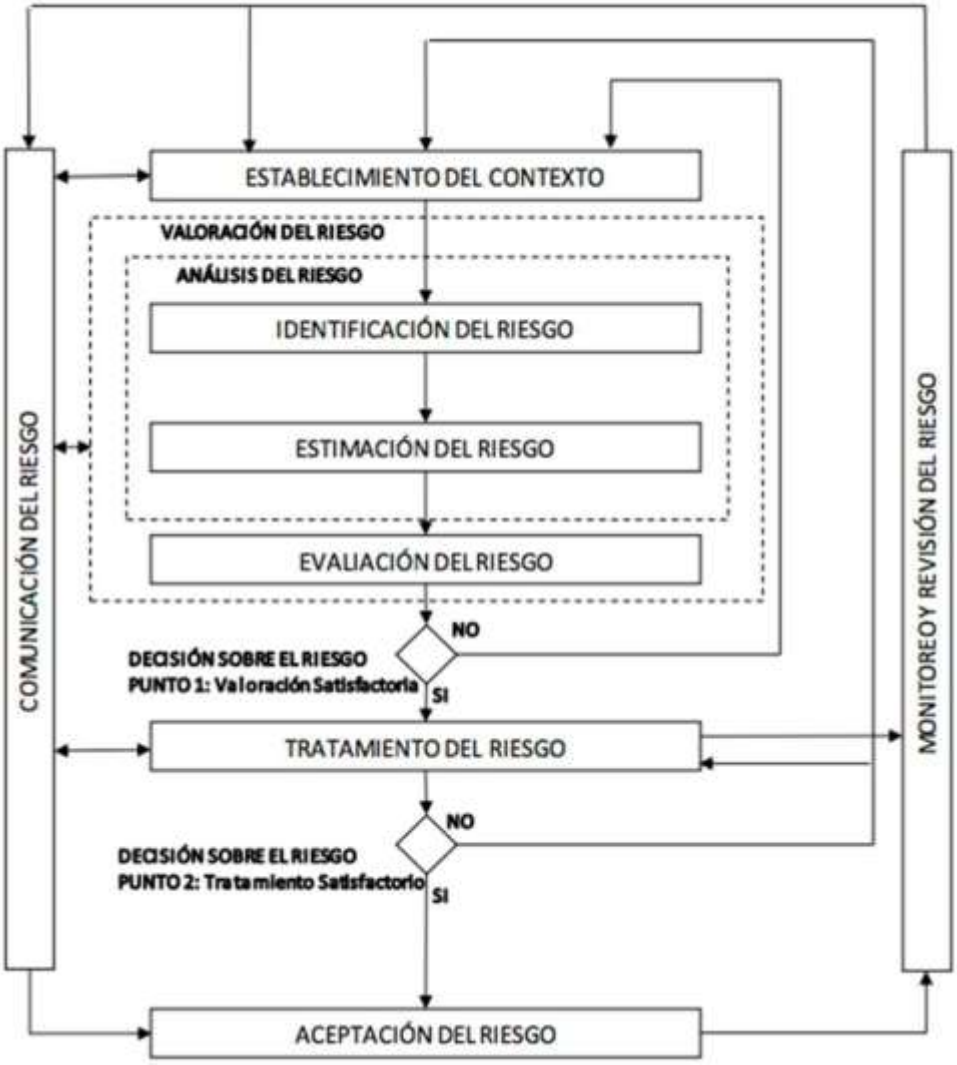
- **Sistema de información**
  Computadoras y redes de comunicaciones electrónicas, datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información.

- **TI**
  Tecnologías de la Información.

- **Trazabilidad**
  Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

- **Vulnerabilidad**
  Cálculo o estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada

6. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Proceso para la administración de riesgos de seguridad y privacidad de la información
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

A continuación, se definen los criterios para el análisis de riesgos, los riesgos que se detecten y trabajarán serán los ubicados en la zona de riesgo extrema.

		IMPACTO				
		1. Insignificante	2. Menor	3. Moderado	4. Mayor	5. Catastrófico
PROBABILIDAD	1. Rara vez	Baja	Baja	Moderado	Alta	Extrema
	2. Improbable	Baja	Baja	Moderado	Alta	Extrema
	3. Posible	Baja	Moderado	Alta	Extrema	Extrema
	4. Probable	Moderado	Alta	Alta	Extrema	Extrema
	5. Casi seguro	Alta	Alta	Extrema	Extrema	Extrema

Identificador	Zona de riesgo	Definición
	Extrema	Es un riesgo que puede representar pérdidas para la Entidad si se materializa con un impacto crítico o grave, y se debe mitigar por medio de planes de acción.
	Alta	Es un riesgo que puede representar pérdidas para la organización si se materializa con un impacto alto y se debe mitigar por medio de planes de acción.
	Moderado	Es un riesgo que representa un nivel moderado y se debe controlar para que no aumente.
	Baja	Es un riesgo que se debe monitorear, pero está dentro de los riesgos para la entidad

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

7.1 cronograma para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Entidad

ID	ACTIVIDAD	Fecha Inicio	Fecha Final
1	Sensibilización institucional sobre política de seguridad de la información	01/02/2025	31/12/2025
2	Desarrollar y/o actualizar el inventario de activos de información de TI	01/02/2025	31/12/2025

3	Elaborar procedimiento gestión de Riesgos de seguridad de la información	01/02/2025	31/12/2025
4	Ejecutar Plan de riesgos de seguridad y privacidad de la información	01/02/2025	31/12/2025

7.2 Plan de riesgos de seguridad y privacidad de la información

ID	ACTIVIDAD	F. INICIO	F. FINAL
1	Identificación de Riesgos	01/02/2025	31/12/2025
2	Evaluación de Controles	01/02/2025	31/12/2025
3	Socialización y Comunicación Política de administración de Riesgos	01/02/2025	31/12/2025