RESOLUCION NO. GE-1000-8-2-018
OCTUBRE 20 DE 2021

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA TERMINAL DE TRANSPORTES DE MANIZALES S.A

EL GERENTE DE LA TERMINAL DE TRANSPORES DE MANIZALES S.A EMPRESA INDUSTRIAL Y COMERCIAL DEL ESTADO, EN USO DE SUS FACULTADES LEGALES Y ESATUTARIAS.

CONSIDERANDO:

Que mediante Decreto 415 del 7 de marzo de 2016, se adiciono al Decreto 1083 de 2015, todo lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la información y las comunicaciones.

Que el Decreto 1078 de 2015 contemplo en el articulo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la Información.

Que mediante el decreto 612 del 4 de abril de 2018 se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del estado.

Que el Decreto 1008 de 14 de junio de 2018 se establece que la seguridad y privacidad de la información es uno de los habilitadores transversales de la nueva política de Gobierno Digital.

Que mediante **el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información** se busca proteger la integridad y garantizar la disponibilidad y confidencialidad de todos los activos de información de la entidad.

Por lo anterior,

RESUELVE

ARTÍCULO PRIMERO. Adoptar el **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información de la Terminal de Transportes de Manizales S.A.,** el cual se adjunta y hace parte integral de la presente resolución.

RESOLUCION NO. GE-1000-8-2-018
OCTUBRE 20 DE 2021

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA TERMINAL DE TRANSPORTES DE MANIZALES S.A

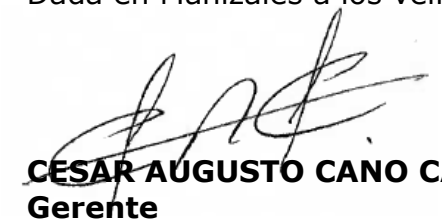
ARTÍCULO SEGUNDO. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información de la Terminal de Transportes de Manizales S.A, tiene como objetivo establecer y aplicar un conjunto de controles para evitar o mitigar los riesgos de seguridad y privacidad que puedan afectar los activos de información de la entidad.

ARTÍCULO TERCERO. La presente Resolución rige a partir de la fecha de expedición.

ARTÍCULO CUARTO. La presente Resolución deberá difundirse a través de los medios de Comunicación interna de **la Terminal de Transportes de Manizales S.A.**

Comuníquese y Cúmplase.

Dada en Manizales a los veinte (20) del mes de octubre de 2021.



CESAR AUGUSTO CANO CARVAJAL
Gerente

Proyecta : Adriana Lucia Naranjo P
Profesional Universitaria
Dependencia de Sistemas

TERMINAL DE TRANSPORTES DE MANIZALES S.A

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

Responsables

ADRIANA LUCIA NARANJO PINEDA
Profesional Universitario
Dependencia de Sistemas

TABLA DE CONTENIDO

1. INTRODUCCION

La gestión del **plan de tratamiento de riesgos de seguridad y privacidad de la información** son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio. Todos los servidores públicos y trabajadores oficiales, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, el presente plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y de una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y de lineamientos sencillos y claros para su adecuada gestión.

Además, teniendo en cuenta el nuevo concepto de Gobierno Digital y la alineación de la Política de Gobierno Digital como una de las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se constituye en el instrumento que soportará el habilitador transversal de la Seguridad de la Información de la Terminal de Transportes de Manizales S.SA., dentro de los instrumentos que apoyan la implementación del MSPI de la Entidad,

2. OBJETIVOS

OBJETIVO GENERAL: Definir las actividades, lineamientos y factores determinantes que permitirán llevar a cabo la gestión para el tratamiento de los riegos de seguridad de la información, identificados en la Terminal de Transportes de Manizales S.A.

OBJETIVOS ESPECÍFICOS

- Definir las actividades requeridas para la implementar al tratamiento de riesgos de seguridad de la información.
- Evaluar el nivel de riesgo actual con el impacto generado después de implementar el plan de tratamiento de riesgos de seguridad de la información.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información.

3. CONTEXTO ESTRATEGICO

El presente plan está alineado y contribuye al logro de la misión, visión y mega meta y demás elementos del direccionamiento estratégico de la Terminal de Transportes de Manizales S.A., los cuales se estipulan en el Plan Estratégico Institucional.

ARTICULACION CON EL CONTEXTO ESTRATEGICO	
APORTES AL DIRECCIONAMIENTO ESTRATEGICO	✓ **Fortalecer los Sistemas Información** ✓ **Fortalecer el uso de las tecnologías de la información** ✓ **Optimizar los procesos misionales** ✓ **Mejorar los procesos administrativos**
GESTION Y DESEMPEÑO INSTITUCIONAL	✓ **Política de Gobierno Digital** ✓ **Política de Seguridad Digital** ✓ **Política de transparencia, acceso a la información publica y lucha contra la corrupción**

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Se define el **Plan de Tratamiento de Riesgos de seguridad y privacidad de la información** como el proceso mediante el cual se identifica, comprende, evalúa, y mitiga cualquier tipo de riesgo o amenaza en la información de una determinada organización. Dentro de dicho plan, se contempla la identificación de activos informáticos, las vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas; lo anterior con el fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

4. ALCANCE

El **Plan de Tratamiento de Riesgos de seguridad y privacidad de la información** es de estricta aplicabilidad y cumplimiento por parte de todos los servidores públicos, trabajadores oficiales y contratistas que presten sus servicios o tengan algún tipo de relación con la Entidad; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por la Terminal de Transportes de Manizales S.A., en especial aquellos que impactan directamente la consecución de los objetivos misionales.

5. TÉRMINOS Y DEFINICIONES.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar su importancia.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Da el resultado en donde se ubica el riesgo por cada activo de información.

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 de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos 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.

Control: Medida que permite reducir o mitigar un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Factores de Riesgo: Son las fuentes generadoras de riesgos, Agente ya sea humano o tecnológico que genera el riesgo

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de exactitud y completitud

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

6. MARCO NORMATIVO

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.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Norma NTC / ISO 27001:2013: Tecnología de la Información. Técnicas de seguridad de la información y Código de Práctica para controles de seguridad de la información.

Ley 44 de 1993: "Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).

Ley 527 de 1999: "Por medio de 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: "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: "Por la cual se dictan disposiciones generales para la protección de datos personales".

Ley 1712 de 2014: "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 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

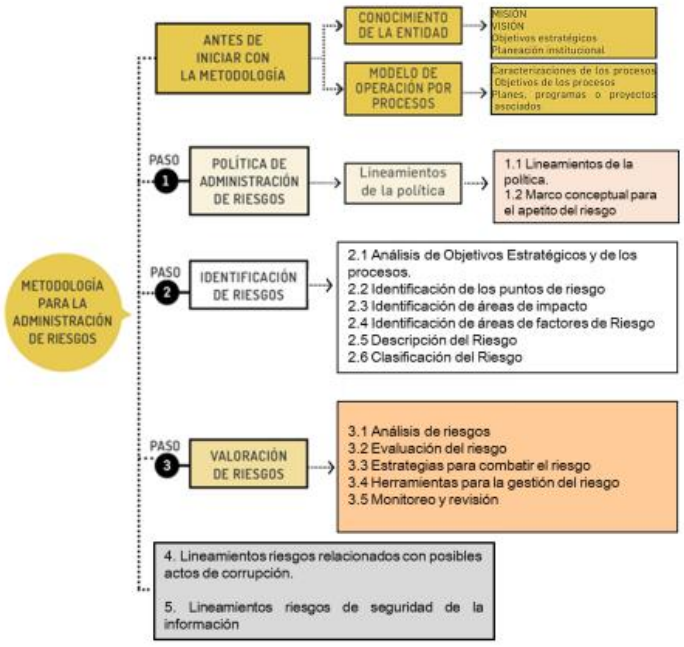
Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Diciembre de 2010, del Departamento Administrativo de la Función Publica.

7. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACION

El desarrollo el **Plan de Tratamiento de Riesgos de seguridad y privacidad de la información**, tiene como propósito es la identificación, estimación y evaluación de los riesgos de **la Terminal de Transportes de Manizales S.A.**, para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos. La Gestión de Riesgos de **la Terminal de Transportes de Manizales S.A.**, incluyendo los Riesgos de Seguridad y Privacidad se lleva a cabo por los Líderes de cada proceso y lo gestionan para el cumplimiento de la misión, visión y objetivos misionales, con el fin de determinar el tratamiento del riesgo aceptable sobre cada uno de los riesgos identificados, teniendo en cuenta el siguiente esquema:

Metodología para la administración de riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Beneficios de la administración en la Gestión de Riesgos

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

La Terminal de Transportes de Manizales S.A., sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de **La Terminal de Transportes de Manizales S.A**., para reducir los niveles de riesgo, es indispensable diseñar un plan de tratamiento de riesgos para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

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

A continuación, cronograma propuesto para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Terminal de Transportes de Manizales S.A., y descripción general de las tareas principales.

CRONOGRAMA DE ACTIVIDADES				
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
ID	ACTIVIDAD	DESCRIPCION	RESPONSABLE	PLAZO 2021 / 2022
1	Sensibilización Plan de Seguridad y Privacidad de la información	Realizar la divulgación del Plan de Seguridad y Privacidad de la información, para el uso de los sistemas y la información, y estos deben ser cumplidos por parte de todos los usuarios del sistema.	Prof. Univ. Dependencia de Sistemas	12/31/2021
2	Desarrollar y/o actualizar el inventario de activos de información	Desarrollar la identificación, clasificación, mantenimiento y actualización del inventario de activos de información de la Terminal	Prof. Univ. Dependencia de Sistemas	01/31/2022
3	Elaborar procedimientos gestión de Riesgos de seguridad de la información	Realizar la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Plan de de Seguridad y Privacidad de la información.	Prof. Univ. Dependencia de Sistemas	01/31/2022
4	Adoptar la metodología para la gestión de los riesgos de seguridad y privacidad de la información	Aplicar la metodología de gestión del riesgo de diciembre de 2020, de la Funcion publica, que permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que esta expuesta la entidad	Prof. Univ. Dependencia de Sistemas	01/31/2022

Manizales, octubre 20 de 2021.