TERMINAL DE TRANSPORTES DE MANIZALES S.A

SI-1600-1-1-010

DEPENDENCIA DE SISTEMAS

DIRIGIDO A:

GERENCIA

ENERO 30 DE 2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PRESENTÓ

ADRIANA LUCIA NARANJO PINEDA
Profesional Universitaria
Dependencia de Sistemas

CONTENIDO

Carrera 43 No. 65-100 Los Cambulos Teléfonos 8785641 – 8787858 – 8787832
Email – gerencia@terminaldemanizales.com.co
www.terminaldemanizales.com.co

INTRODUCCIÓN

La Terminal de Transportes de Manizales S.A., Sociedad Comercial Anónima conformada entre Entidades Públicas, entidad descentralizada por servicios encargada del transporte público interdepartamental, intermunicipal y veredal de pasajeros del Municipio de Manizales, con el propósito de salvaguardar la información para el mejoramiento y la toma de decisiones en el direccionamiento estratégico y garantizando la seguridad de los datos y el cumplimiento de las normas legales, propone el siguiente Plan de Seguridad y Privacidad de la Información para la vigencia 2024.

En atención a lo anterior, la entidad y de acuerdo con los lineamientos de la Política de Gobierno Digital, reglamentada a través del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, que en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, y de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información y en cumplimiento de la normativa aplicable vigente, y en particular, como parte de los planes institucionales establecidos en el Decreto 612 de 2018 y en cumplimiento del 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”

1. OBJETIVOS

1.1 *OBJETIVO GENERAL*

Definir las acciones para garantizar la confidencialidad, integridad y disponibilidad y privacidad de la información de **La Terminal de Transportes de Manizales S.A.**, de acuerdo con las estrategias de Gobierno Digital, Modelo Integrado de Planeación y Gestión- MIPG, requerimientos de la entidad y disposiciones legales vigentes.

1.2 *OBJETIVOS ESPECÍFICOS*

- Fortalecer y optimizar la gestión de seguridad y privacidad de la información al interior de **La Terminal de Transportes de Manizales S.A.**, apoyando el cumplimiento de los objetivos estratégicos de la entidad.
- Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información de **La Terminal de Transportes de Manizales S.A.**
- Establecer políticas de seguridad y privacidad de la información de **La Terminal de Transportes de Manizales S.A.**
- Identificar los niveles de cumplimiento y alcance de las políticas de seguridad y privacidad de la información.
- Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la información.

2. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información aplica a todos los procesos definidos en **La Terminal de Transportes de Manizales S.A.**, donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

Las Políticas y lineamientos de seguridad definidos en la actualización del plan de seguridad y privacidad de la información 2023, deben ser conocidos, difundidos y cumplidos por los funcionarios, contratistas y todos los terceros que tengan acceso, almacenen, procesen, consulten o trasmitan información de la Entidad.

3. MARCO NORMATIVO

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".

Decreto 19 de 2012: "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".

Decreto 1377 de 2013: "Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015**".**

Decreto 886 de 2014: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

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 1081 de 2015: "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."

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 415 de 2016: (Por el cual se adiciona el Decreto 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.)

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

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 612 de 2018: (Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.)

Ley 1915 de 2018: (Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en Materia de Derecho de Autor y Derechos Conexos.)

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

4. 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.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

Administración de Riesgo: Actividad encaminada a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

Análisis de Riesgo: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del 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.

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.

Causas: Medios, circunstancias, situaciones o agentes generadores del evento.

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.

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

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

Consecuencia: Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

Control: Acciones encaminadas a educir la probabilidad de ocurrencia o el impacto que pueda generar la materialización de un riesgo.

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

Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los proyectos de inversión y las actividades críticas de control de los procesos.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestor del Riesgo: funcionario líder de la dependencia, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación no deseada.

Impacto: Magnitud de las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos por proceso, haciendo la descripción de cada uno de ellos, las posibles consecuencias y su forma de tratamiento.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad 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, ejemplo, mediante una matriz de Probabilidad - Impacto.

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.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Política de manejo del Riesgo: Son los Criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar los riesgos de la entidad, en función de su evaluación.

Privacidad de datos: La privacidad de datos, también llamada protección de datos es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros

Probabilidad: Medida para estimar la posibilidad de que ocurra un evento.

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Responsable del Riesgo: Es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo Residual: Es aquel que continúa aún después de aplicar controles para mitigar el riesgo.

Riesgo Inherente: Es el riesgo puro, al cual no se han aplicado controles, para controlar y buscar evitar su materialización.

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.

Rol: Papel, función que alguien o algo desempeña.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y

recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Tratamiento 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.

Valoración: Grado de exposición al riego con la clasificación de probabilidad e impacto aplicando los controles existentes.

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

5. POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

La Terminal de Transportes de Manizales S.A., en el marco de sus funciones, se compromete a proteger y asegurar la información tanto física como digital, a través de acciones, estrategias y recursos necesarios, con el fin de cumplir con los requisitos legales y reglamentarios de la entidad, buscando fortalecer y mejorar el Plan de Seguridad y Privacidad de la información y sus objetivos.

6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- ✓ Implementar y fortalecer los controles para la protección de los activos de información.
- ✓ Prevenir la materialización de los riesgos de seguridad de la información identificados.
- ✓ Controlar y minimizar los incidentes de Seguridad de Información.
- ✓ Cumplir los requisitos normativos, legales y de seguridad de la información, a través de políticas, lineamientos, guías y directrices del Sistema de Gestión de Seguridad de la Información SGSI.
- ✓ Generar una cultura en seguridad de la información.
- ✓ Evaluar y mejorar el Sistema de Gestión de Seguridad de la Información, con el fin de lograr la eficiencia y su mejora continua.

7. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

7.1 JUSTIFICACIÓN

La Terminal de Transportes de Manizales S.A., busca salvaguardar la información en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información, con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de Seguridad de la información física y digital de acuerdo a la caracterización de los Usuarios tanto internos como externos.

7.2 OBJETIVO DE IMPLEMENTACIÓN DE LA POLÍTICA

Definir los mecanismos y todas las medidas necesarias por parte de **la Terminal de Transportes de Manizales S.A.,** tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

7.3 ALCANCE

Una política de seguridad y privacidad es una regla de definición general, independiente de los ambientes tecnológicos y físicos, que representa los objetivos sobre los que se sustenta el Sistema de Gestión de Seguridad de la Información.

El enunciado y la definición de estos lineamientos, comprende todos los aspectos administrativos y de control que deben ser acatados por el personal que labora para **la Terminal de Transportes de Manizales S.A.,** con el fin de lograr un adecuado nivel de cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

La política de seguridad y privacidad es de obligatorio cumplimiento para todos los servidores públicos y contratistas que presten sus servicios o tengan algún tipo de relación con la Entidad; así como a los espacios

físicos del mismo que conlleven un componente de seguridad de información.

A continuación, se establecen las políticas sobre las cuales se debe direccionar el plan de seguridad y privacidad de la información, en **la Terminal de Transportes de Manizales S.A.**

8. POLITÍCAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA TERMINAL DE TRANSPORTES DE MANIZALES S.A

8.1 POLÍTICA DE ROLES Y RESPONSABILIDADES

Disposiciones generales:

Los directivos, servidores públicos, contratistas, proveedores y terceros deben:

Hacer buen uso de la información que es generada resultado de las actividades laborales.

Almacenar la información resultado del ejercicio de las funciones en la carpeta local o servidor de archivos designado por la Dependencia de Sistemas, de esta forma se garantiza las copias de respaldo, de lo contrario no queda dentro de la presente política.

En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados.

Todos los activos de información deben tener un propietario, custodio y deben estar debidamente identificados.

Los propietarios de los activos de información son los responsables de aplicar y velar por el cumplimiento de los controles que garanticen la disponibilidad, confidencialidad e integridad de la información de los activos.

Se deben definir los roles y privilegios de la plataforma tecnológica y sistemas de información, de acuerdo a los perfiles y necesidades de uso dentro de su rol en la entidad.

Se debe seguir los procedimientos definidos por la Dependencia de Sistemas en los Sistemas de Información.

Se debe informar a todos los directivos, servidores públicos, contratistas, proveedores y terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad, solicitantes de accesos a componentes tecnológicos y sistemas de información sobre el uso y la responsabilidad que tienen al ser autorizados.

8.2 POLÍTICA GESTIÓN DE ACTIVOS DE INFORMACIÓN

Todo computador tiene recursos limitados (memoria, disco duro) que deberán ser aprovechados para actividades relacionadas con el trabajo del usuario. Está prohibido utilizar estos recursos para actividades que no tengan relación alguna con la función en la Terminal.

A los funcionarios se les asignará una estación de trabajo que puede estar compuesta por (Equipo, impresora, scaner, u otros), los cuales se les asignará en el inventario y del cual será responsable de su uso y protección diaria.

Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias, verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

Tanto los directivos, servidores públicos, contratistas, proveedores y terceros deben asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

Los usuarios deberán apagar correctamente sus equipos y/o estaciones de trabajo al retirarse de la oficina o puesto de trabajo.

8.3 *POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED*

La Dependencia de Sistemas, debe asegurar que las redes inalámbricas de **La Terminal de Transportes de Manizales S.A.,** cuenten con métodos de autenticación que evite accesos no autorizados. La Dependencia de Sistemas, debe establecer controles para la identificación y autenticación de los usuarios que requieran hacer uso de los recursos de red de **La Terminal de**

Transportes de Manizales S.A., así como velar por la aceptación de las responsabilidades de dichos terceros.

La Dependencia de Sistemas debe verificar el acceso de los usuarios a los sistemas de información, con el fin de validar que los usuarios tengan acceso permitido, únicamente, a aquellos recursos de red y servicios de la plataforma tecnológica y sistemas de información para los que fueron autorizados.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a recursos de red, y servicios de la plataforma tecnológica y sistemas de información de **La Terminal de Transportes de Manizales S.A.,** deberán autenticarse, y la Dependencia de Sistemas deberá verificar su acceso.

Los servidores públicos, contratistas, proveedores y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad son responsables de hacer buen uso de los recursos tecnológicos de **La Terminal de Transportes de Manizales S.A.,** y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros, servidores públicos y Terceros.

Cualquier requerimiento que tenga un usuario respecto a instalación, desinstalación, o actualización de sus aplicaciones, deberá solicitarse por medio de la Mesa de Ayuda a la Dependencia de Sistemas y estas entraran a ser evaluadas para su aprobación o denegación.

Si un equipo de cómputo requiere seguir algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño que haya sufrido, se debe realizar una solicitud a la Mesa de Ayuda de la Dependencia de Sistemas, la cual respaldará la información y documentos que se consideren de las funciones asignas a su cargo.

8.4 *POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS*

La Dependencia de Sistemas, debe definir lineamientos para la configuración de Contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de **La Terminal de Transportes de Manizales S.A.,** dichos lineamientos deben considerar aspectos como cambio periódico, bloqueo, inactivación y cambio de contraseña en el primer acceso, entre otros.

La Dependencia de Sistemas, deberá asegurarse de la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, o cambian de cargo.

Los servidores públicos, contratistas, proveedores y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún

tipo de relación con la Entidad deben hacerse responsables de las acciones realizadas sobre la plataforma tecnológica y sistemas de información de **La Terminal de Transportes de Manizales S.A.,** así como del usuario y contraseña asignados para el acceso a los recursos informáticos y de información de la entidad.

Los servidores públicos, contratistas, proveedores y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad no deben compartir sus cuentas de usuarios y contraseñas con terceras personas. Las cuentas de usuarios y contraseñas son intransferibles y solo pueden ser usadas por la persona autorizada y para fines institucionales.

8.5 *POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y APLICATIVOS*

Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

La Dependencia de Sistemas, asignara los accesos a los sistemas y aplicativos de la Terminal de Transportes de Manizales S.A., bajo cuentas de usuarios y contraseñas, las cuales son intransferibles y solo pueden ser usadas por la persona autorizada y para fines institucionales.

El ingreso de dispositivos CD's, memorias UBS, discos duros externo, u otro dispositivo de almacenamiento, conteniendo información o software, deberá ser vacunado con el antivirus que posee la entidad, antes de abrir su contenido, por los servidores públicos que hagan uso de los elementos antes descritos.

Sólo el personal autorizado por la Dependencia de Sistemas podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la entidad; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la entidad.

8.6 *POLÍTICAS DE SEGURIDAD FÍSICA*

La Terminal de Transportes de Manizales S.A., provee los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus dependencias. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las dependencias destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido y **La Terminal de**

Transportes de Manizales S.A., deberá contar con mecanismos de seguridad física y control de acceso.

Las solicitudes de acceso al área donde se encuentra Cuarto de Servidores y/o Centros de Cableado deben ser aprobadas por funcionarios que apoyan la Dependencia de Sistemas, no obstante, los visitantes y/o terceras partes siempre deberán estar acompañados de un funcionario.

La Dependencia de Sistemas, debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

La Dependencia de Sistemas debe garantizar que el Cuarto de Servidores y/o Centros de Cableado, que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.

8.7 *POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS*

La Dependencia de Sistemas, debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de las plataformas tecnológicas de la entidad, redes de datos, equipos de cómputo y demás dispositivos disponibles al servicio de **La Terminal de Transportes de Manizales S.A.**

La Dependencia de Sistemas, debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los servidores públicos de la Terminal, ya sea cuando son dados de baja o cambian de usuario.

La Dependencia de Sistemas, realizara el acompañamiento para realizar movimientos y asignaciones de recursos tecnológicos; en caso de ser necesario, y estos deberán ser informados oportunamente a la Dependencia de Servicios Administrativos y Comunicaciones, para lo que corresponda a su asignación y responsable.

Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de **La Terminal de Transportes de Manizales S.A.**, el usuario responsable debe informar La Dependencia de Sistemas, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por La Dependencia de Sistemas.

Los servidores públicos, contratistas, y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad y que hagan uso de los equipos de cómputo no deberán manipular el registro del sistema operativo, ni realizar ninguna modificación en los archivos de configuración.

Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados en lugares públicos o a la vista, en el caso de que estén siendo transportados.

Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

En caso de pérdida o robo de un equipo de cómputo, se deberá proceder según lo establecido en el Manual de Inventaros vigente de la entidad.

Los servidores públicos, contratistas, proveedores y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad deberán asegurar que se guarden en sitios seguros, los equipos de cómputo como portátiles, discos duros, memorias u otros dispositivos, una vez sean utilizados durante el desarrollo de jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

Se distribuirá, en la medida de los posible, fundas y/o forros para los equipos y/o estaciones de trabajo, para que los usuarios dejen los equipos correctamente cubiertos durante el tiempo que permanezcan inactivos.

8.8 *POLÍTICA DE USO ADECUADO DE INTERNET*

La Dependencia de Sistemas, debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de accesos establecidos.

El uso de internet es únicamente para actividades relacionadas con las funciones del negocio, manteniéndose las restricciones de seguridad establecidas por la entidad.

El uso de servicios de mensajería instantánea solo se utilizará para actividades de la entidad y el acceso a las redes sociales estará autorizado solo a un grupo restringido de usuarios teniendo en cuenta su perfil.

La Dependencia de Sistemas, debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

La Dependencia de Sistemas, debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

Los usuarios del servicio de Internet de **La Terminal de Transportes de Manizales S.A.**, deben hacer uso de este en relación con las actividades laborales que así lo requieran.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

El uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Instagram y otros similares, solo se utilizará para actividades de la entidad y el acceso estará autorizado solo a un grupo restringido de usuarios teniendo en cuenta su perfil.

Aquellos usuarios que tengan permiso para acceder a Internet a través de las redes de la Terminal, deberán tener cuidado con la difusión de su identificación como son usuario y clave de los sistemas de información que se manejan al interior de la Terminal.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

No está permitido el intercambio no autorizado de información de propiedad de **La Terminal de Transportes de Manizales S.A.**, por parte de los servidores públicos con terceros.

Las estaciones de trabajo, servidores, y equipos portátiles, deberán contar con la configuración correspondiente de acuerdo con la configuración de la seguridad perimetral aprobada para los activos de información de cada dependencia.

8.9 *POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN*

La Dependencia de Sistemas, debe disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de **La Terminal de Transportes de Manizales S.A.**

La Dependencia de Sistemas, deben garantizar la ejecución periódica de los Procedimientos de Copia de Respaldo y Restauración de la Información de **La Terminal de Transportes de Manizales S.A.**

La Dependencia de Sistemas, debe definir y aprobar los tiempos en que se efectuarán las actividades de copia de respaldo y restauración de la información de **La Terminal de Transportes de Manizales S.A.**

La Dependencia de Sistemas, debe monitorear periódicamente, el cumplimiento de las actividades de generación de copias de respaldo de la información institucional y el ejercicio de restauración de esta, para verificar el estado en que se encuentra.

La Dependencia de Sistemas, debe disponer de los recursos tecnológicos necesarios, para permitir la identificación y disposición de los medios de almacenamiento, que soportarán las copias de seguridad de la información de la entidad.

Para el retiro de un servidor público de la entidad se realiza Backus de la información por parte de La Dependencia de Sistemas tan pronto se reciba el portátil o equipo asignado por la entidad. Además, se realiza el cambio o la cancelación de la cuenta en el directorio activo y en los aplicativos de los sistemas de información que se tenían asignados.

8.10 *POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES*

Las dependencias y sedes administrativas de **La Terminal de Transportes de Manizales S.A.**, que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

Las dependencias que procesan datos personales de usuarios, servidores públicos, contratistas, proveedores u otras terceras partes deben asegurar:

- Que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

- Deberán establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

- Deberán acoger las directrices y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

- La Terminal de Transportes de Manizales S.A., deberá implantar los controles necesarios para proteger la información personal de los usuarios, servidores públicos, contratistas, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

8.11 *POLÍTICA DE CONTINUIDAD, CONTINGENCIA Y RECUPERACIÓN DE LA INFORMACIÓN*

La Dependencia de Sistemas debe garantizar que los Procedimientos de Contingencia, Recuperación y Retorno a la Normalidad, incluyan las consideraciones de seguridad de la información necesaria y requerida, para el cumplimiento de los objetivos trazados.

9. CUMPLIMIENTO

El cumplimiento del Plan de Seguridad y Privacidad de la Información es obligatorio. Si los servidores públicos y contratistas que presten sus servicios o tengan algún tipo de relación con la Entidad, violan este plan, **La Terminal de Transportes de Manizales S.A.,** se reserva el derecho de tomar las medidas correspondientes.

10. COMUNICACIÓN

Mediante la socialización a todos los servidores públicos, contratistas, proveedores y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad, se dará a conocer el contenido del documento del Plan de Seguridad y Privacidad de la Información.

Todos los servidores públicos, contratistas, proveedores y/o terceros de **La Terminal de Transportes de Manizales S.A.,** que presten sus servicios o tengan algún tipo de relación con la Entidad, deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, el cual estará publicado en la página web de la entidad http://www.terminaldemanizales.com.co.

¿QUÉ SE COMUNICA?	¿PARA QUÉ LO COMUNICA?	¿RESPONSABLE DE LA INFORMACIÓN A COMUNICAR?	¿CÓMO LO COMUNICA?	¿A QUIÉN LO COMUNICA?	¿CUÁNDO LO COMUNICA?
Plan de Seguridad y Privacidad de la Información	Para garantizar la confidencialidad, Integridad y disponibilidad de la Información en l entidad.	Profesional Universitaria Dependencia de Sistemas	Capacitaciones, campañas, publicación en carteleras, plegables, correo electrónico, página web	Servidores Públicos, Contratistas, proveedores y/o terceros	Permanentemente

11. CRONOGRAMA DE ACTIVIDADES

TERMINAL DE TRANSPORTES DE MANIZALES S.A

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

No.	ACTIVIDADES	VIGENCIA 2024												
		Meta	Fecha de Reporte o Ejecución de la actividad											PRODUCTO / EVIDENCIA
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
1	Actualizar el Plan de Seguridad y Privacidad de la Información para la vigencia 2024	100%	X												Presentar para aprobación el Plan de Seguridad y Privacidad de la Información vigencia 2024
2	Realizar socialización del Plan de Seguridad y Privacidad de la Información vigencia 2024	100%				X									Realizar socialización del Plan de Seguridad y Privacidad de la Información de la vigencia 2024
3	Realizar seguimiento a las Políticas del Plan de Seguridad y Privacidad de Información	100%						X							Realizar seguimiento al cumplimiento de las Politicas del Plan de Seguridad y Privacidad de la Información de la vigencia 2024
4	Realizar capacitación a los funcionarios de la entidad en temas de seguridad de la información.	100%							X						Realizar capacitación a los funcionarios de la Terminal, acerca del cumplimiento de las Politicas del Plan de Seguridad y Privacidad de la Información
5	Realizar la programación del plan anual de mantenimientos preventivos de la infraestructura Tecnológica	100%	X												Realizar la Programación del Plan anual de mantenimientos preventivos de la infraestructura Tecnológica vigencia 2024
6	Ejecutar el Plan anual de mantenimientos preventivos de la infraestructura Tecnológica de la entidad	100%	X	X	X	X	X	X	X	X	X	X	X	X	Ejecutar el Plan anual de mantenimientos preventivos de la infraestructura Tecnológica vigencia 2024
7	Realizar contratación de los proyectos de gasto e inversión planteados para la vigencia 2024, teniendo en cuenta los lineamientos del manual de contratación	100%	X		X				X						Celebrar los contratos de gastos e inversión vigencia 2024, teniendo en cuenta los lineamientos de la entidad
8	Realizar la actualización del inventario de equipos de computación y comunicación	100%				X									Realizar la actualizacion de los Inventario de equipos de computación y comunicación
9	Actualizar inventario de activos de la información y su clasificación	100%					X								Presentar para aprobación el inventario de activos de la información y su clasificación vigencia 2024
10	Levantar catálogo de servicios de TI	100%					X								Presentar para aprobación el catálogo de servicios de TI vigencia 2024
11	Levantar el catálogo de componentes de información.	100%						X							Presentar para aprobación el catálogo de componentes de información vigencia 2024

Responsable : Adriana Lucia Naranjo Pineda. Profesional Universitaria. Dependencia de Sistemas

12. INDICADOR

Número de actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información desarrolladas / Número total de actividades del plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información desarrolladas *100. **Periodicidad**. Semestral.

13. VIGENCIA

El Presente Plan de Seguridad y Privacidad de la Información, entra en vigor a partir de su adopción y publicación.

Manizales, enero 30 de 2024.