Contenido

1. INTRODUCCIÓN

El presente manual se convierte en el marco de referencia de buenas prácticas, lineamientos, controles, entre otros aspectos que permiten promover comportamientos seguros y proteger la información de la Terminal de Transporte de diferentes amenazas del entorno en cuanto a la seguridad informática, entornos físicos y los recursos que custodian esta información, mantener los principios propios, de igual forma establecer pautas claras y medidas de protección.

2. OBJETIVO GENERAL

El presente documento tiene como objetivo fundamental, comunicar a todos los trabajadores de planta, en misión, socios de negocios, contratistas, proveedores, clientes, visitantes, y partes interesadas, la política de seguridad de la información y ciberseguridad y políticas específicas establecidas por la Terminal de Transporte S.A., que permitan proteger la información de la entidad, así como estar alineados con la política de tratamiento de datos personales, sin importar el medio por el cual sea administrada, distribuida o almacenada, todo ello con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y de sus activos relacionados.

3. TÉRMINOS RELEVANTES

- **ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN**: En relación con seguridad de la información, Recursos del sistema de información o relacionados con éste, necesarios para que la Terminal de Transporte S.A. funcione correctamente y alcance los objetivos propuestos por la dirección.
- **AMENAZA:** fenómeno o proceso natural o causado por el ser humano que puede poner en peligro a un grupo de personas, sus cosas y su ambiente.
- **CIBERSEGURIDAD**: es la práctica de proteger sistemas, redes y programas de ataques digitales.
- **CLASIFICACIÓN DE LA INFORMACIÓN**: Es la decisión para asignar un nivel de sensibilidad a los datos cuando se están creando, corrigiendo, almacenando o transmitiendo. Un esquema de clasificación debe usarse para definir un conjunto apropiado de niveles de protección y comunicar las medidas especiales de tratamiento.
- **CÓDIGO MALICIOSO:** El software malicioso incluye todos los programas (incluyendo macros y scripts) que se codifican deliberadamente para causar un acontecimiento inesperado en el PC de un usuario.
- **CUSTODIO DE LOS ACTIVOS DE INFORMACION**: Empleados que administran el almacenamiento de los activos de información y encargados de implementar los controles de seguridad definidos por los responsables de los activos de información.
- **INTELIGENCIA ARTIFICIAL**: Se relaciona con la concentración o en la que la tecnología o los equipos informáticos pueden tomar decisiones en función de los datos.
- **ISO 27001:2022**: Estándar que especifica los requerimientos para implementar un sistema de gestión de seguridad de la información.

- **PLAN DE CONTINUIDAD DEL NEGOCIO (BCP):** Procedimientos establecidos para recuperar y restaurar las funciones críticas del negocio parcial o totalmente interrumpidas.
- **RESPONSABLE DE LOS ACTIVOS DE INFORMACION**: Empleado designado por la gerencia de la Terminal de Transporte S.A., encargado de inventariar, clasificar y proteger los activos de información bajo su responsabilidad y controlar permanentemente que se cumplan las restricciones de acceso y otros controles de seguridad de la información.
- **SEGURIDAD DE LA INFORMACIÓN**: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; otras características también pueden estar involucradas, tales como la autenticidad, responsabilidad, aceptabilidad, confiabilidad y no repudio.
- **USUARIO DE LA INFORMACIÓN**: Son usuarios de información todas las personas que, directa o indirectamente, tengan algún tipo de relación con ella y tienen acceso al uso de los recursos tecnológicos de la entidad. Tomando en cuenta esta definición, son usuarios: los empleados, proveedores, contratistas, aprendices, socios de negocio, entre otros.

4. NORMATIVIDAD APLICABLE

- Reglamento interno del trabajo de la Terminal de Transporte S.A.
- Resolución 115 de septiembre 2017 y 32 de noviembre 2020 de la Terminal de Transporte S.A. en la cual indican las funciones del comité SIG respecto al Subsistema en particular y la generalidad del SIG.
- Resolución 99 de diciembre de 2022 de la Terminal de Transporte S.A.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
- NTC – ISO/IEC 27001:2022
- CONPES 3995 Política nacional de confianza y seguridad digital

5. COMPROMISO DE MEJORA CONTINUA

a. Las políticas de seguridad de la Terminal de Transporte S.A. dan cumplimiento a la norma NTC ISO 27001:2022.
b. El director de recursos tecnológicos es responsable por la actualización permanente estas políticas y normas de seguridad. La actualización se debe dar en la medida en que ocurra uno de los siguientes eventos:
   - Cambios en el ambiente de negocios o estrategia empresarial (ejemplo: nuevas estrategias de mercado, nuevos productos, cambios de prioridades, fusiones o cesiones, cambios en la estructura organizacional, nuevas dependencias o áreas, etc.)
   - Cambios en la infraestructura de riesgos de seguridad de información de la Terminal de Transporte S.A. Estos cambios pueden ser como consecuencia de un análisis de riesgos y vulnerabilidades o por la aparición de nuevas vulnerabilidades y/o amenazas que cambien el perfil de riesgo de la infraestructura técnica de la organización.
   - Cambios en versiones de estándares buenas prácticas que sean viables en su implementación.
   - Nuevas obligaciones legales, comerciales y/o reglamentarias o cambio de las existentes que afecten el procesamiento de la información, intercambio o custodia de información de terceros.

- Los cambios o actualizaciones se presentarán en el informe a la gerencia

6. MECANISMOS DE COMUNICACIÓN

Se implementarán mecanismos de comunicación para garantizar la importancia de la política de seguridad de la información en Capacitaciones al personal, campañas de comunicación a través de los medios internos establecidos para tal fin. Estas actividades se llevarán a cabo de manera presencial o remota y se tomaran las respectivas listas de asistencia y evaluaciones que permitan evaluar la efectividad e interiorizaron de los temas vistos. Todas estas actividades serán presentadas junto con los indicadores en el informe de gestión a la gerencia.

7. POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

La Terminal de Transporte SA, consciente de la responsabilidad de proteger la información almacenada en sus sistemas y la que se encuentra de manera física, establece los siguientes lineamientos como política de Seguridad de la Información, alineados a la política de protección de datos personales, en procura de dar respuesta a los requisitos de protección de sus activos de información y minimizar los riesgos por pérdida de confidencialidad, disponibilidad e integridad de la información, estableciendo los siguientes lineamientos para este fin:

- Se Promueve la implementación de una cultura de seguridad de la información y buenas prácticas a fin de garantizar que la confidencialidad, integridad y disponibilidad de la información, esté presente en todas las actividades que realiza la Terminal de Transporte de Bogotá S.A.
- Cumplir con los requisitos de marco legal y regulaciones en materia de protección de datos personales, las que apliquen en materia de seguridad informática y de manejo responsable de información propia y de nuestros clientes.
- Gestionar los riesgos de seguridad de la información, manteniéndolos en niveles aceptables de riesgo residual.
- Prevenir, controlar, mitigar amenazas que generen impactos que afecten la infraestructura de trabajo a fin de dar continuidad permanente a nuestros servicios.
- Identificar oportunidades de mejora del subsistema de gestión de seguridad de la información para lo cual se garantizan los recursos necesarios para el mantenimiento del subsistema de Seguridad de la Información de la Terminal de Transporte integrado a todos los procesos organizacionales.

8. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Comprometer a todo el personal de la Terminal con el Sistema de Gestión de Seguridad de la Información, en adelante SGSI, con el fin de que éste sea eficaz a la hora de preservar la seguridad digital y de la información y sus activos asociados.
- Establecer un esquema de seguridad digital, ciberseguridad, y de protección de datos, transparente y aplicable bajo la responsabilidad de la Terminal en cuanto a la administración del riesgo se refiere.

- Proteger la información y recursos tecnológicos utilizados por la Terminal frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.
- Establecer las directrices para el uso de los componentes de hardware, software, información física e información digital de la Terminal, con el fin de mitigar los riesgos de ocurrencia de incidentes de seguridad de la información.
- Proteger los activos de información de la Terminal, de tal manera que se garantice su confidencialidad, integridad y disponibilidad de acuerdo con el nivel de criticidad establecido en la clasificación y valoración de dichos activos.

9. ALCANCE

Las políticas, normas y procedimientos que hacen parte de este documento son de obligatorio cumplimiento para todos los trabajadores de planta, consultores externos, socios de negocios, proveedores, contratistas, personal en misión, terceros que presten sus servicios o tengan alguna relación con la entidad y Clientes de La Terminal de Transporte S.A. Este documento describe las políticas de seguridad de la información definidas por la Terminal, teniendo en cuenta la estrategia de Gobierno Digital de Ministerio de las TIC, la ley estatutaria de protección de datos personales (Ley 1581 de 2012) y sus decretos reglamentarios, lineamientos de la norma NTC – ISO/IEC 27001:2022 y documento CONPES 3995 Política nacional de confianza y seguridad digital y demás legislación aplicable.

10.POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

10.1. Política para la gestión segura de documentos

Para todas las actividades de la Terminal se establecen las actividades de control que deben ser implementadas para el manejo responsable de documentación física o digital independientemente de su lugar de almacenamiento. Esta política tiene como finalidad establecer las directrices para proteger la información contra uso no autorizado, divulgación o publicación, modificación, daño o pérdida y establecer el cumplimiento de reglamentaciones y leyes aplicables a la Terminal de Transporte S.A. Cada Líder de Área establece criterios de seguridad de las siguientes actividades para dar cumplimiento a la política de seguridad de la información.

- Se debe tener en cuenta el procedimiento de etiquetado de documentación para identificar la clasificación de información y las responsabilidades que se deben tener en cuenta en cuanto a los accesos se refiere a información sensible de la Terminal de Transporte. Es necesario definir quién tiene acceso a los documentos y cómo se controla ese acceso, incluyendo la autenticación de usuarios y la asignación de permisos.
- No está autorizada la salida de información ni física ni digital sin las debidas autorizaciones de salida por parte de los líderes de cada una de las áreas.
- El préstamo de documentos por parte de archivo será controlado para su devolución respectiva y será solicitado a través de los líderes de cada una de las áreas de la terminal.

- No está autorizado la destrucción de información cuando se trate de las versiones definitivas, si la misma no cuenta con la evidencia de la gestión realizada por parte de los líderes que son los responsables o custodios de la misma.
- Definir los plazos para conservar los documentos y los métodos seguros para eliminarlos cuando ya no sean necesarios según los requisitos del área de Archivo, en los procesos y procedimiento del Área de archivo y el manejo de las tablas de retención documental, de manera que estos procesos estén sincronizados con los requisitos de confidencialidad, integridad y disponibilidad documental establecidos por la política de seguridad de la información y sus respectivos controles.
- Establece medidas para proteger físicamente los documentos en archivos seguros o sistemas de almacenamiento protegidos.
- Es necesario gestionar las versiones de los documentos, evitando la pérdida de datos o la confusión sobre qué versión es la más reciente.
- Gestionar el manejo de llaves de escritorios y archivadores para conservar la información segura
- Asegurar que la política cumpla con las regulaciones y normativas aplicables en materia de privacidad y seguridad de la información.
- Control de llaves: los encargados serán el personal de archivo de cada sede, es responsabilidad del personal de archivo conservar las llaves, no sacar duplicados sin previa autorización y asegurar el buen manejo.
- Acceso de ingreso por medio de la tarjeta: las tarjetas para el ingreso al área de archivo se deben solicitar por parte del profesional de archivo por medio de un correo dirigido al coordinador terminales satélites, quien será el encargado de la asignación y administración de las mismas.
- Para garantizar un acceso seguro y controlado a las áreas de archivo, todas las personas que no pertenezcan al área de archivo y que necesiten ingresar deben diligenciar el formato 'Formato de ingreso áreas archivo'. Durante la visita, el personal externo que acceda a estas áreas deberá estar acompañado en todo momento por un miembro del personal del archivo.
- Establecer procedimientos para realizar copias de seguridad periódicas de los documentos y garantizar su recuperación en caso de pérdida o daño.

10.2. Política de intercambio de información

Para todas las actividades de la terminal que involucren entrega de información física o digital se tomarán en cuenta los siguientes lineamientos:

- Se debe proteger la información confidencial contra intercepción, copia, modificación o destrucción para los cual se debe etiquetar la misma.
- Se deben implementar mecanismos para detectar software malicioso que pueda ser transmitido.
- Informar a todos los empleados y externos sus responsabilidades con el cumplimiento de las políticas y procedimientos para el intercambio de información.
- Concienciar a los empleados y terceros acerca de las precauciones que deben tener cuando exponen información confidencial en conversaciones personales o telefónicas.
- Concienciar a los empleados y terceros en que no deben dejar mensajes con información confidencial en ningún tipo de contestador o buzón telefónico, ni enviarla a través de aplicaciones de mensajería electrónica.

- Se deben controlar los riesgos relacionados con el envío de información confidencial por medio de las conexiones inalámbricas.
- Realizar acuerdos sobre transferencia de información con proveedores y terceros de manera cifrada.
- El intercambio de información con terceros se debe realizar exclusivamente si existen razones del negocio.
- El intercambio de información clasificada como confidencial con un tercero, debe ser aprobado por el dueño de la información.
- Se deben definir claramente los responsables del envío, recepción y notificación del intercambio de información.
- Se deben definir los acuerdos de retención de dicha información.
- Establecer las responsabilidades de derechos de autor y licenciamiento.
- Las transferencias de información solamente serán realizadas por los medios autorizados por la Terminal de Transporte. No está autorizado para el intercambio de información dispositivos externos, redes sociales, correos personales entre otros medios, para realizar esta actividad a menos de que se solicite por medio escrito y autorizado por los respectivos líderes al Director de recursos tecnológicos, el cual realizará las respectivas evaluaciones de criterio de riesgos y configuraciones de seguridad para el monitoreo de actividades.
- Para el intercambio seguro de la información física, es necesario tener en cuenta el procedimiento de préstamo y/o consulta de documentos, el cual establece protocolos para garantizar que la información sea manejada de manera segura y solo por personas autorizadas. Es importante que el acceso a la información física esté restringido y que solo aquellos que hayan sido autorizados por el líder del área correspondiente puedan acceder a ella.

10.3. Política de control de acceso

El acceso lógico a todos los sistemas de información de La Terminal de Transporte S.A. debe ser controlado mediante un sistema de autenticación y autorización con el fin de prevenir el acceso no autorizado a la información confidencial de la organización y sus clientes a través de los siguientes lineamientos:

10.3.1. Control de Acceso a redes y servicios de red y aplicaciones:

- El acceso a las redes de comunicaciones y servicios de red de La Terminal de Transporte debe estar controlado por medio de mecanismos de autenticación y autorización.
- Los sistemas de autenticación y autorización para los servidores de red y aplicativos deben estar conformados por un usuario y una contraseña.
- Los privilegios de acceso de los usuarios a los servicios de red y sistemas de información deben ser autorizados por los dueños de la información y deben limitarse al mínimo requerido para cumplir con las responsabilidades propias de su cargo tal como se establece en el procedimiento de control de acceso.

10.3.2. Gestión de acceso de usuarios para el Registro y cancelación de usuarios:

- El Director de Recursos Tecnológicos debe implementar un procedimiento formal y documentado para la creación, modificación y eliminación de usuarios en los diferentes sistemas de información. Este procedimiento debe incluir:
- La autorización por parte del dueño de la información para obtener acceso a los diferentes sistemas de información.
- Verificación que el acceso concedido es el solicitado, el autorizado y el apropiado de acuerdo al objetivo del negocio y la política de menor privilegio.
- El acceso a los diferentes sistemas de información no se debe otorgar hasta que el procedimiento de creación no se realice totalmente y el usuario confirme el recibo a satisfacción.
- El Director de Gestión Humana o el supervisor del contrato debe informar a la Dirección de Recursos Tecnológicos los empleados que se han retirado de la organización para que se proceda con la eliminación de sus usuarios y accesos a los diferentes sistemas de información y servicios de red.
- El Director de Gestión Humana, o el supervisor del contrato debe informar a la Dirección de Recursos Tecnológicos los empleados que no requieren el acceso a los sistemas de información por un periodo de tiempo determinado.
- La Dirección de Recursos Tecnológicos debe eliminar o inhabilitar el acceso a los sistemas de información o servicios de red (intranet, internet, correo) cuando un empleado, cliente, proveedor o consultor externo se retire o termine sus relaciones contractuales con la organización.
- Está totalmente prohibido que las áreas utilicen los usuarios de empleados que se encuentren ausentes de la Terminal de Transporte S.A. En caso de que se requiere el acceso a un aplicativo, es necesario hacer la solicitud formal para otro empleado mediante el procedimiento establecido.
- Cuando un empleado cliente, proveedor o consultor externo cambia de cargo al interior de la organización, se deben eliminar o reasignar sus privilegios de acceso, de acuerdo con lo establecido en el formato de gestión de roles y perfiles de cada área.
- La Gerencia de la Terminal de Transporte S.A. debe garantizar la segregación de funciones en las actividades de autorización, asignación, creación y administración de credenciales en los diferentes sistemas de información.
- La Dirección de recursos tecnológicos debe entregar de manera segura las contraseñas de inicio de sesión de los diferentes servicios de red y aplicativos a los usuarios solicitantes.
- Los aplicativos y servicios de red deben obligar a los usuarios el cambio de su contraseña de inicio de sesión la primera vez que ingresan al sistema.
- El acceso a los repositorios de los usuarios y contraseñas en los diferentes aplicativos, sistemas de información y sistemas operativos debe ser estrictamente controlado y asignado única y exclusivamente a los usuarios que lo requieren para desarrollar sus actividades por medio de autorización escrita del líder de cada área.
- Los repositorios que contienen la información de usuarios y contraseñas de los aplicativos y sistemas operativos deben ser cifrados.
- El transporte por la red de la información de usuarios y contraseñas se debe realizar por medio de mecanismos de cifrado de información.

10.3.3. Gestión de derechos de acceso privilegiado

- Los perfiles con acceso privilegiado o perfiles de administración en los diferentes sistemas de información, aplicativos y servicios de red de La terminal de Transportes deben ser asignados por el Director de Recursos Tecnológicos, única y exclusivamente a los usuarios que lo requieren para desarrollar sus actividades y responsabilidades.
- Los usuarios con perfil de administración que vienen por defecto en los sistemas operativos, aplicativos y servicios de red solo pueden ser utilizados en caso de contingencia.
- Las actividades de los usuarios con perfiles de administración deben ser registradas en un log de auditoría.
- La asignación de privilegios en los sistemas de información debe ser aprobadas por los dueños o responsables de la información y se deben basar en la política de menor privilegio.
- El director de Recursos Tecnológicos con el apoyo de los dueños o responsables de la información debe crear la matriz de roles y perfiles de seguridad, en donde se detallen los privilegios que deben tener los perfiles de usuarios en cada uno de los sistemas de información.
- Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes (cargos); estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios (política de menor privilegio). Los permisos de acceso a los aplicativos deben ser garantizados por cargos y no por empleados.
- El acceso a los datos almacenados en las bases de datos se debe realizar exclusivamente por los aplicativos.
- Si se requiere acceso y/o modificación de datos por medio de comandos SQL y/u otros ejecutados directamente sobre los motores de base de datos, estas modificaciones deben ser autorizadas por los dueños de la información mediante un procedimiento formal y se debe dejar un registro de auditoría que detalle la transacción realizada, fecha, hora y usuario que la realiza.
- Se guardará en caja fuerte la última versión de la contraseñas de superusuario y la revisión de esta actividad se consigna con acta de asignación al responsable Si el mismo cambia se debe realizar por escrito la reasignación y actualización de este recurso.

10.4. Política de uso de servicios de nube

- Todos los procesos que actualmente se encuentren administrados desde aplicativos que se encuentren en nube se debe garantizar la seguridad de los datos, cumplimiento normativo, privacidad de la información en términos de los perfiles de acceso a la información.
- Cada proveedor de estos servicios debe presentar las políticas respectivas las cuales deben ser presentadas y los mecanismos de seguridad implementados, así como los respectivos informes de gestión de monitoreo y control.
- La alta dirección es responsable de garantizar que se establezcan y mantengan controles adecuados para proteger la información confidencial y cumplir con los requisitos legales y regulatorios pertinentes.

- Los propietarios de información son responsables de utilizar los servicios de nube de manera segura, así como de informar cualquier incidente de seguridad o preocupación al oficial de seguridad de la información.
- Realizar copias de seguridad regulares de los datos almacenados en la nube y probar la capacidad de restauración de las mismas de manera mensual.
- Se debe evaluar los riesgos antes de la adopción de cualquier servicio de nube para determinar la adecuación y la seguridad del proveedor.
- Se deben establecer acuerdos formales de confidencialidad con los proveedores de servicios de nube en donde se especifiquen las responsabilidades y el cumplimiento en los requisitos de seguridad.
- Se debe implementar controles de acceso adecuados para garantizar que solo los usuarios autorizados tengan acceso a los datos almacenados en la nube.
- Gestionar la generación de los informes de capacidad y monitoreo de seguridad de manera que se detecten amenazas en forma oportuna.
- Se deben cifrar los datos confidenciales en reposo y en tránsito utilizando algoritmos robustos y prácticas de cifrado recomendadas.
- Gestionar los incidentes de seguridad de manera integral con los involucrados del servicio y el proveedor.

10.5. Política de Protección de registro

- Todos los procesos críticos en los sistemas informáticos estarán monitoreados mediante la recolección, almacenamiento y acceso a los registros de actividades o eventos dentro de un sistema o plataforma en donde se incluya según sea el caso información de acciones realizadas por usuarios, eventos de seguridad, o cambios en la configuración además de definir quién tiene autorización para acceder a ellos y con qué propósito.
- Es necesario realizar copias de seguridad de los registros con accesos limitados implementado los mecanismos de retención y disposición segura de acuerdo a los requisitos legales y regulatorios
- Los registros deben ser clasificados y etiquetados según su nivel de confidencialidad e importancia.
- Se deben establecer controles de acceso adecuados para limitar el acceso a los registros de seguridad solo a nivel de super usuarios o usuarios autorizados.
- Se debe garantizar la integridad de los registros mediante la implementación de mecanismos de protección contra modificaciones no autorizadas.
- Se debe identificar e implementar un monitoreo continuo de los registros y establecer sus amenazas o actividades sospechosas.
- Se deben establecer procedimientos claros para la gestión de incidentes relacionados con la seguridad de los registros.
- Se debe establecer procedimientos para el manejo de los incidentes incluyendo la notificación oportuna a las partes interesadas afectadas.

10.6. Política específica sobre privacidad y protección de la Información Personal PII

Se encuentra alineada con la política de protección de datos personales de la Terminal de trasporte de Bogotá publicada en la página web https://www.terminaldetransporte.gov.co/la-entidad/transparencia-y-acceso-a-la-informacion-publica/politica-de-tratamiento-de-datos-personales/

10.7. Política de teletrabajo

La Terminal de Transporte S.A establece las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la entidad; así mismo, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

- Para la modalidad de trabajo remoto (Teletrabajo) para los funcionarios de la Terminal de Transporte S.A., debe tener la autorización respectiva de la Dirección de Gestión Humana.
- Las funciones y actividades que se realizan en modalidad de Teletrabajo deben ser aprobadas y formalizadas por la Dirección de Gestión Humana de la Terminal de Transporte S.A
- El jefe inmediato del teletrabajador, debe aprobar el plan de trabajo a desarrollar en esta modalidad, el cual debe estar alineado con el rol habitual del funcionario e indicadores que evidencien su cumplimiento.
- La Dirección de Gestión Humana, en coordinación con la Dirección de Recursos Tecnológicos, deben definir los controles informáticos y reportes para que se garantice que el funcionario cumpla el horario laboral, desde el lugar asignado o la aplicación del procedimiento y cumplimiento de condiciones pactadas.
- Los usuarios como los equipos que se dispongan para esta modalidad deben mantener en idénticas condiciones a los que operan en la red local, cumpliendo con las Políticas del Manual de Seguridad de la Información.
- La Dirección de Recursos Tecnológicos, debe garantizar que el teletrabajador tenga acceso a las aplicaciones requeridas para sus funciones a desarrollar, según solicitud realizada por la Dirección de gestión humana.
- La Dirección de recursos tecnológicos coordinará y validará la implementación de los recursos tecnológicos necesarios para uso de esta modalidad de trabajo y debe aplicar controles de seguridad al medio de comunicación que se establezca para el acceso remoto, hacia la infraestructura tecnológica de La Terminal de Transporte S.A.
- El oficial de seguridad de la información debe realizar un seguimiento a los sistemas, equipos, flujo de información y funcionarios en modalidad de teletrabajo para el monitoreo de la seguridad de la información.

10.8. Política de escritorio limpio y pantalla limpia

- Los empleados, clientes, proveedores o consultores externos deben garantizar que la información clasificada confidencial en medios digitales como físicos que no estén siendo utilizada por personal

autorizado, debe permanecer siempre bajo llave y no debe ser desatendida en ninguna ubicación no controlada.

- Todos los empleados que tengan bajo su responsabilidad información confidencial deben contar con un archivador con llave para guardar todo el material sensible (material impreso, en medios magnéticos) y una copia de la llave debe ser entregada a la Dirección del área.
- Todos los empleados deben evitar que los Equipos desatendidos queden al alcance de personal no autorizado al acceso de esta información.
- Es responsabilidad de todos hacer buen uso de los servicios de impresión de la entidad por lo que los documentos impresos se deben recoger de este dispositivo sin ser abandonados y únicamente utilizados con mecanismos de autenticación.
- Cuando un empleado se retire temporalmente de su puesto de trabajo, debe hacer un logout de la sesión del aplicativo y activar el bloqueo del escritorio de trabajo del computador mediante la opción de protector de pantalla.
- La opción de protector de pantalla de Windows debe configurarse con la Activación del protector de pantalla después de cinco minutos de inactividad del computador.
- El desbloqueo de computador requiere contraseña de red.
- Toda estación de trabajo debe tener configurado el papel tapiz institucional.
- Los escritorios de los computadores deben estar despejados no debe estar a la vista documentos editables ni sensibles.

10.9. Política contra los riesgos de la utilización de dispositivos móviles

El uso de dispositivos móviles o de almacenamiento externo en los diferentes equipos de cómputo, unidades de red compartidas y servidores de la Terminal, constituyen una herramienta que sirve para la extracción rápida y directa de información entre los funcionarios de la Terminal que a la vez puede exponer información confidencial y sensible de la Terminal a diversos riesgos y peligros.

La TERMINAL es consciente que este tipo de herramientas o dispositivos externos son muy útiles para el desarrollo normal de sus labores diarias, pero igualmente son herramientas que permiten copiar información sin dejar huella física ni registro de dicha acción.

Por lo anterior la TERMINAL DE TRANSPORTE S.A., define esta Política, para asegurarse que la información propietaria, adquirida o puesta en custodia en la TERMINAL no está expuesta a uso no autorizado, divulgación o pérdida, modificación, fuga, y que esta debe ser protegida adecuadamente según su confidencialidad, importancia y valor.

Es así que, la Dirección de Recursos Tecnológicos, con el propósito de dar cumplimiento a los objetivos de Gobierno en Línea en lo que respecta a la implementación del Modelo de Seguridad de la Información, determina la presente Política que define el manejo y limitaciones de este tipo de dispositivos móviles o externos. Se prohíbe el uso indebido de dispositivos de almacenamiento externo para:

- Utilizar dispositivos de almacenamiento móviles o externo con el fin de almacenar, transportar o exponer información privada, sensible, confidencial o reservada de la Terminal de Transporte S.A.
- Ejecutar cualquier tipo de programa no autorizado por la Dirección de Recursos Tecnológicos desde cualquiera dispositivo de almacenamiento externo
- Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos
- No obstante, lo anterior, se hace claridad que, para el cumplimiento de sus funciones y los objetivos de la Terminal, la Gerencia General autorizara el uso de los dispositivos móviles o de almacenamiento externo.

10.10. Política de Copias de Seguridad

- La Dirección de Recursos Tecnológicos debe respaldar con copias de seguridad la información Institucional que sea de misión crítica, dichas copias deben ser tomadas y probadas de acuerdo con el procedimiento FTI- PR02 Backup y Recuperación de la Información.
- La Dirección de Recursos Tecnológicos debe garantizar copia de las bases de datos del software que utiliza, dichas copias deben ser tomadas y probadas de acuerdo procedimiento FTI-PR02 Backup y Recuperación de la Información.
- Es responsabilidad exclusiva de los usuarios, que, para la creación de copias de seguridad de archivos usados, custodiados o producidos por esto, deben tener en cuenta que esta información se debe alojar en la carpeta MIS DOCUMENTOS.
- Los dueños de la información deben garantizar que se realiza Backup a toda la información sensible almacenada en los servidores de red.
- La Dirección de Recursos Tecnológicos debe establecer una estrategia de Backup de información crítica que soporte los requerimientos de recuperación y continuidad de La Terminal de Transporte S.A.
- Los requerimientos que se deben tener en cuenta en la estrategia de respaldo de información son:
  - Información crítica a la que se debe realizar copia de seguridad.
  - Nivel de confidencialidad de la información respaldada.
  - Periodicidad de la generación de copias de seguridad (tener en cuenta el RPO del plan de continuidad del negocio).
  - Periodo de retención.

- Es responsabilidad del director de Recursos Tecnológicos de la Terminal de Transporte S.A. la supervisión periódica de los procesos de toma de Backup, rotación y custodia de estos.
- Mensualmente, se deben realizar pruebas de restauración de un Backup para verificar el contenido y la usabilidad del mismo.

10.11. Política sobre el uso de los controles criptográficos

- La dirección de recursos tecnológicos gestionará la protección de llaves criptográficas definición de protocolos y mecanismos de almacenamiento.
- Los usuarios finales deben dar el uso, protección adecuada y aplicar los controles necesarios para evitar accesos no autorizados a las llaves criptográficas asignadas.
- Se debe distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
- La dirección de Recursos Tecnológicos es el custodio de los certificados de seguridad de los servicios que se exponen en internet y que son propiedad de la Entidad.

10.12. Política de propiedad intelectual

- Todas las actividades asociadas a la propiedad intelectual serán establecidas de manera contractual en los que se debe fijar la fecha de inicio de propiedad los derechos establecidos.
- Todos los derechos de propiedad intelectual existentes antes de la fecha de celebración de un contrato pertenecerán a la parte que era dueña de tales derechos.
- Los derechos morales de autor sobre los trabajos que elabore un contratista o tercero en desarrollo del objeto de un contrato pertenecerán a él y en este sentido se considerara como autor moral de los mismos, conforme a lo previsto en el artículo 30 de la Ley 23 de 1982.
- Los derechos patrimoniales de autor, desarrollos tecnológicos, patentes, propiedad industrial y sus derivados que se generen con ocasión de los entregables, productos, trabajos, escritos, documentos, artículos, investigaciones, programas, desarrollos y en general cualquier creación de un contratista o tercero que surja por motivo de la ejecución de un contrato corresponderá en su totalidad a la Terminal de transporte de conformidad con lo previsto en el artículo 20 de la Ley 23 de 1982 modificado por el artículo 28 de la Ley 1450 de 2011, sin que haya lugar a reconocimiento económico distinto al pago del valor previsto por su contrato.
- Queda entendido y así lo acepta tanto el contratista o tercero como la Terminal de transporte que los derechos patrimoniales de los trabajos que surjan de la prestación del servicio encargado o producto de un contrato, corresponden a la Terminal de transporte.
- Toda especificación, dibujo, bosquejo, modelo, muestra, herramienta, dato, documentación, programa de computación o información técnica o comercial suministrada o revelada entre los acuerdos que realice la terminal con sus terceros por motivo o con ocasión de las actividades derivadas de la ejecución de un contrato, es de propiedad exclusiva de quien ejerza derechos sobre la misma, incluyendo la titularidad correspondiente a los derechos de autor, las marcas, lemas, emblemas, denominaciones y patentes, entre otros, asociados con el objeto del presente contrato, los equipos y todo material susceptible de tales derechos, que aporten cada uno según sea el caso
- Todo material tangible debe ser devuelto a la respectiva parte que lo aporta, a la finalización de las actividades de un contrato. La autorización de uso de marcas, lemas, emblemas, denominaciones y patentes, entre otras, no otorga derecho a la otra parte, más allá de lo expresamente señalado en el contrato. Dicha autorización está limitada al cumplimiento de las

actividades derivadas del mismo y no se hace extensiva a terceros. Bajo ningún concepto ni la Terminal ni el Tercero o Proveedor pueden usar el nombre, los signos distintivos, marcas o los símbolos que identifiquen a la otra, a menos que haya recibido previamente autorización por escrito para tales efectos.

10.13. Política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida

- Generación segura de llaves: el área de Gestión de la información y las comunicaciones establece los procedimientos para generar llaves cifradas de manera segura, utilizando métodos criptográficamente sólidos y generadores de números aleatorios confiables.
- Define cómo deben almacenarse las llaves cifradas para evitar accesos no autorizados, como utilizar sistemas de gestión de claves seguros y protegidos por contraseñas fuertes.
- Establece protocolos para la distribución segura de llaves a los usuarios autorizados, evitando la divulgación no autorizada o el acceso indebido.
- Implementa un proceso para la rotación regular de llaves, con el fin de limitar la exposición a posibles ataques y mantener la seguridad a largo plazo.
- Establece mecanismos de monitoreo para rastrear el uso de las llaves cifradas y detectar posibles anomalías o intentos de acceso no autorizado.
- Asegurar que la política cumpla con las regulaciones y estándares de seguridad de la información aplicables, según sea necesario.

11.REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN:

- El Director de Recursos Tecnológicos (Oficial de Seguridad de la Información) debe revisar periódicamente el cumplimiento de las políticas, normas y procedimientos de seguridad de la información. En caso de identificar incumplimiento de las mismas, se debe iniciar el procedimiento de gestión de incidentes de seguridad.
- Los Subgerentes, directores y jefes de las áreas de La Terminal de Transporte S.A. deben reportar al Oficial de Seguridad de la información cuando se observe incumplimiento de las políticas y/o normas de seguridad de la información.
- Los directores y jefes de las áreas de la Terminal de Transporte S.A. deben revisar regularmente los procedimientos de su área para asegurar que se cumplen razonablemente.
- El Director de Recursos Tecnológicos (Oficial de Seguridad de la información) debe verificar que los directores y jefes de las áreas de las diferentes áreas gestionen adecuadamente el cumplimiento de las normas y procedimientos de seguridad de la información.