**Contenido** Pág.

**INTRODUCCIÓN** ..... 6
**1. OBJETIVO GENERAL** ..... 6
**2. OBJETIVOS ESPECIFICOS** ..... 6
**3. ALCANCE** ..... 6
**4. TÉRMINOS RELEVANTES** ..... 7
**5. NORMATIVIDAD APLICABLE** ..... 7
**6. RESPONSABILIDADES Y AUTORIDAD ASOCIADAS A SEGURIDAD DE LA INFORMACIÓN** ..... 8
**6.1. REVISIÓN Y ACTUALIZACIÓN DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN DELA TERMINAL DE TRANSPORTE S.A.** ..... 9
**7. NORMAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN DE LA TERMINAL DE TRANSPORTE S.A.** 9
**7.1. ORGANIZACIÓN DE LA TERMINAL DE TRANSPORTE S.A. PARA LA SEGURIDAD DE LA INFORMACIÓN** ..... 9
**7.1.1. Roles y responsabilidades para con la seguridad de la información** ..... 9
**7.1.2. Segregación de tareas** ..... 12
**7.1.3. Contacto con autoridades** ..... 12
**7.1.4. Contacto con grupos de interés** ..... 12
**7.1.5. Gestión de proyectos** ..... 12
**7.1.6. Normas de seguridad relacionadas con dispositivos móviles** ..... 12
**7.1.7. Política de teletrabajo** ..... 13
**8. SEGURIDAD DEL RECURSO HUMANO** ..... 14
**8.1. PROCESO DE INGRESO** ..... 14
**8.1.1. Antes de la contratación** ..... 14
**8.1.2. Durante el periodo de vinculación contractual con la Terminal de Transporte S.A.** ..... 14
**8.1.3. Cese o cambio de puestos de trabajo** ..... 15
**8.2. GESTIÓN DE ACTIVOS DE INFORMACIÓNPolítica para el manejo de la información** ..... 15
**8.2.1. Responsabilidad sobre los activos** ..... 16
**8.2.1.2. Propiedad de los activos** ..... 16
**8.2.2. Clasificación de la información** ..... 16
**8.2.3. Etiquetado de la información** ..... 17
**8.2.4. Manejo de información** ..... 18
**8.2.5. Manejo de medios de almacenamiento** ..... 18

COPIA CONTROLADA

**8.3. GESTIÓN DE CONTROL DE ACCESOS LÓGICOS ..... 19**
**8.3.1. Requisitos del negocio para el control de acceso lógico a la información: ..... 19**
**8.3.1.1. Política de control de acceso ..... 19**
**8.3.1.2. Acceso a redes y servicios de red ..... 19**
**8.3.2. Gestión de acceso de usuarios: ..... 19**
**8.3.2.1. Registro y cancelación de usuarios ..... 19**
**8.3.2.2. Suministro de acceso de usuarios ..... 20**
**8.3.2.3. Gestión de derechos de acceso privilegiado ..... 20**
**8.3.2.4. Gestión de la información de autenticación secreta de usuarios: ..... 21**
**8.3.2.5. Revisión de los derechos de acceso de los usuarios: ..... 22**
**8.3.2.6. Retiro o ajuste de los derechos de acceso: ..... 22**
**8.3.3. Control de acceso a sistemas y aplicaciones: ..... 22**
**8.3.3.1. Restricción de acceso a la información ..... 22**
**8.3.3.2. Procedimiento de acceso seguro ..... 22**
**8.3.3.3. Gestión de contraseñas ..... 22**
**8.3.3.4. Programas utilitarios privilegiados ..... 23**
**8.3.3.5. Control de acceso a código fuente ..... 23**
**8.4. POLITICA SOBRE CONTROLES CRIPTOGRÁFICOS ..... 23**
**8.5. GESTIÓN DE SEGURIDAD FÍSICA Y AMBIENTAL ..... 23**
**8.5.1. Áreas Seguras: ..... 23**
**8.5.1.1. Perímetro de seguridad física: ..... 24**
**8.5.1.2. Controles físicos de entrada: ..... 24**
**8.5.1.3. Protección contra amenazas externas y ambientales: ..... 24**
**8.5.1.4. Trabajo en áreas seguras: ..... 24**
**8.5.2. Seguridad de los equipos ..... 25**
**8.5.2.1. Ubicación de sistemas críticos ..... 25**
**8.5.2.2. Equipos de respaldo ..... 25**
**8.5.2.3. Seguridad en el cableadoPolítica de Instalación de Cableado ..... 25**
**8.5.2.4. Mantenimiento de los equipos: ..... 26**
**8.5.2.5. Salida de activos: ..... 26**
**8.5.2.6. Seguridad de los equipos y activos fuera de las instalaciones de La Terminal de TransporteS.A.: 26**
**8.5.2.7. Reutilización o retirada segura de dispositivos de almacenamiento: ..... 26**

COPIA CONTROLADA

**8.5.2.8. Equipos desatendidos: ..... 26**
**8.5.2.9. Política de puesto de trabajo despejado: ..... 27**
**8.6. SEGURIDAD EN LAS APLICACIONES ..... 27**
**8.6.1. Responsabilidades y procedimientos de operación: ..... 27**
**8.6.1.1. Documentación de procedimientos de operación: ..... 27**
**8.6.1.2. Gestión de cambios: ..... 27**
**8.6.1.3. Gestión de capacidades: ..... 28**
**8.6.1.4. Separación de entornos de desarrollo, pruebas y producción: ..... 28**
**8.6.2. Protección contra código malicioso: ..... 29**
**8.6.3. Copias de seguridad: ..... 29**
**8.6.4. Registro y seguimiento: ..... 30**
**8.6.4.1. Registro de eventos: ..... 30**
**8.6.4.2. Protección de la información de Registro de eventos: ..... 31**
**8.6.4.3. Protección de la información de Registro de eventos ..... 31**
**8.6.4.4. Sincronización de relojes ..... 31**
**8.6.5. Control de sistemas operativos ..... 31**
**8.6.6. Gestión de las vulnerabilidades técnicas ..... 31**
**8.6.7. Controles de auditoría de información ..... 32**
**8.7. SEGURIDAD EN LAS TELECOMUNICACIONES ..... 32**
**8.7.1. Gestión de la seguridad en las redes ..... 32**
**8.7.1.1. Controles de redes ..... 32**
**8.7.1.2. Seguridad en los servicios de red ..... 32**
**8.7.1.3. Normas en el uso de internet ..... 32**
**8.7.1.4. Normas de uso del correo electrónico ..... 33**
**8.7.1.5. Separación en la red. ..... 34**
**8.7.2. Transferencia de información: ..... 34**
**8.7.2.1. Políticas y procedimientos de transferencia de información ..... 34**
**8.7.2.2. Acuerdos sobre trasferencia de información ..... 34**
**8.8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN ..... 35**
**8.8.1. Requisitos de seguridad de los sistemas de información: ..... 35**
**8.8.1.1. Análisis y especificación de los requisitos de seguridad ..... 35**
**8.8.1.2. Seguridad de las comunicaciones en servicios accesibles por redes publicas ..... 35**

COPIA CONTROLADA

**8.8.1.3. Desarrollo contratado externamente ..... 35**
**8.8.1.4. Pruebas de los sistemas y paso a producción..... 36**
**8.9. SEGURIDAD EN LAS RELACIONES CON TERCEROS ..... 37**
**8.9.1. Relaciones con los proveedores..... 37**
**8.9.1.1. Seguridad de la información en la relación con proveedores ..... 37**
**8.9.1.2. Tratamiento de la seguridad en los acuerdos con proveedores..... 37**
**8.9.2. Gestión de la presentación de servicios de proveedores..... 38**
**8.9.2.1. Seguimiento y revisión de los servicios de los proveedores..... 38**
**8.9.2.2. Gestión de cambios en los servicios de los proveedores ..... 38**
**8.10. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN..... 38**
**8.10.1. Responsabilidades y procedimientos:..... 38**
**8.10.2. Notificación de los eventos de seguridad de la información:..... 38**
**8.10.3. Notificación de puntos débiles de seguridad: ..... 39**
**8.10.4. Recopilación de evidencias:..... 39**
**8.11. POLÍTICA ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO 39**
**8.12. CUMPLIMIENTO NORMATIVO..... 40**
**8.12.1. Cumplimiento de los requisitos legales y contractuales: ..... 40**
**8.12.1.1. Derechos de propiedad intelectual (DPI) ..... 40**
**8.12.1.2. Protección de datos y privacidad de la información personal:..... 40**
**8.12.1.3. Prevención del uso inadecuado de los recursos de procesamiento de información:..... 40**
**8.12.1.4. Revisiones de la seguridad de la información: ..... 41**

COPIA CONTROLADA

Lista de Tablas

Pág.

Tabla 1. Comité SIG 10

Lista de Cuadros

Pág.

Cuadro 1. Comité de Sistema Integrado de Gestión 8

COPIA CONTROLADA

## INTRODUCCIÓN

Las políticas se convierten en el marco de referencia de las buenas prácticas, en este caso, aplica para promover los comportamientos seguros alrededor de la seguridad informática manteniendo los principios propios.

## 1. OBJETIVO GENERAL

El presente documento tiene como objetivo fundamental, comunicar a todos los empleados, socios de negocios, proveedores, clientes y visitantes, las políticas y normas de seguridad digital y de la información establecidas por la Terminal de Transporte S.A., para proteger la información sin importar el medio por el cual sea administrada, distribuida o almacenada, garantizando la confidencialidad, integridad y disponibilidad de la información y de sus activos relacionados.

## 2. OBJETIVOS ESPECIFICOS

- 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 y de la información claro, 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.

## 3. ALCANCE

Las políticas, normas y procedimientos que hacen parte de este documento son de obligatorio cumplimiento para todos los empleados, consultores externos, socios de negocios, proveedores, contratistas, personal en misión, terceros que presten sus servicios o tengan alguna relación con la entidad y Clientesde La Terminal de Transporte S.A. Describe las políticas de seguridad digital y de la información definidas por la Terminal, teniendo en cuenta la estrategia de Gobierno Digital de MinTic, la ley estatutaria de protección de datos personales (Ley 1581 de 2012) y sus decretos reglamentarios y demás legislación aplicable, además de la norma NTC – ISO/IEC 27001 :2013.

COPIA CONTROLADA

## 4. 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.
- 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 27001:2013: 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.

## 5. NORMATIVIDAD APLICABLE

- Norma ISO/IEC 27001:2013
- 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”

COPIA CONTROLADA

## 6. RESPONSABILIDADES Y AUTORIDAD ASOCIADAS A SEGURIDAD DE LA INFORMACIÓN

Cuadro 1. Responsabilidades y autoridad en seguridad de la información

| CARGO | PRINCIPALES RESPONSABILIDES |
|---|---|
| Director de Recursos Tecnológicos | Es responsable por la actualización publicación y comunicación de la presente política.<br><br>Nivel de autoridad:<br>Decisiones consultadas: Todas aquellas situaciones en las cuales se presenten sucesos extraordinarios y/o desviaciones en el cumplimiento de sus funciones y responsabilidades, que impliquen riesgo de negocio e impacto económico o administrativo en la organización.<br><br>Decisiones autónomas: Todas las que garanticen el cumplimiento de las políticas y en general el propósito y mejora del Sistema Integrado de Gestión – SIG, fortalecimiento de la cultura de gestión por procesos, documentación implementada en la organización, sus responsabilidades y funciones. |
| Gerente General: | Nivel de autoridad:<br>Decisiones consultadas: Decisiones que impacten económica, reputacional, jurídica y administrativamente a la organización en las cuales, de acuerdo con los Estatutos de la entidad y el Certificado de existencia y representación legal, deban ser llevadas ante la Junta Directiva y Asamblea de accionistas.<br><br>Decisiones autónomas: Todas las que garanticen el cumplimiento de las metas de la organización, su objeto social, propósito y mejora del Sistema Integrado de Gestión - SIG, procesos a su cargo y cumplimiento de sus funciones y responsabilidades. |
| Comité de Sistema Integrado de Gestión | Cumplimiento a lo dispuesto en el artículo cuatro Res. 115 de 2017 funciones del comité del Sistema integrado de Gestión (SIG) en particular el numeral g. Coordinar las revisiones independientes a las políticas de seguridad de la información, y la efectividad y eficiencia de los controles implementados.<br>* Asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;<br>* Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información. |
| Usuarios | • Cumplir y acatar las normas, políticas y estándares de seguridad de la información e informar al Oficial de seguridad de la información cualquier incumplimiento o debilidades de seguridad identificadas.<br>• El usuario y la contraseña son de uso personal e intransferible, no se deben prestar o proporcionar a nadie bajo ninguna circunstancia.<br>• Mantener la confidencialidad del usuario y la contraseña<br>• Evitar la escritura de las contraseñas en papeles<br>• Cambiar la contraseña si tiene algún indicio de su vulnerabilidad |

COPIA CONTROLADA

| | |
|---|---|
| | • No utilizar contraseñas que estén asociadas con temas de la Organización, números de cedula, direcciones, fechas de cumpleaños, películas o palabras que se encuentren en diccionarios.<br>• Cambiar periódicamente las contraseñas<br>• Cambiar las contraseñas la primera vez que inicia sesión.<br>• No incluir las contraseñas en ningún procedimiento automático de conexión, scripts, Shell o mecanismos de recordar contraseñas de navegadores.<br><br>Decisiones Autónomas: Todas las que garanticen el cumplimiento de las políticas y en general documentación implementada en la organización, sus responsabilidades y funciones |

Fuente. Dirección de Recursos Tecnológicos

### 6.1. REVISIÓN Y ACTUALIZACIÓN DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN DE LA TERMINAL DE TRANSPORTE S.A.

a. Las políticas de seguridad de la Terminal de Transporte S.A. dan cumplimiento a la norma NTC ISO 27001:2013.
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:

i. 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.)
ii. 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.
iii. 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.

## 7. NORMAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN DE LA TERMINAL DE TRANSPORTE S.A.

### 7.1. ORGANIZACIÓN DE LA TERMINAL DE TRANSPORTE S.A. PARA LA SEGURIDAD DE LA INFORMACIÓN

#### 7.1.1. Roles y responsabilidades para con la seguridad de la información

a. El articulo cuatro de la resolución 115 de 11 de septiembre de 2017 “Por el cual se crea el Comité Integrado de Gestión SIG (SIG), anti trámites y de Gobierno en línea (GEL) de la Terminal de Transporte S.A. y se dictan otras disposiciones”, indica las funciones del Comité de sistema Integrado de Gestión (SIG) relacionadas a la seguridad de la información y a otros sistemas el cual estará integrado por los siguientes trabajadores:

COPIA CONTROLADA

Tabla 1. Comité SIG

| Integrante |
|---|
| Gerente General o su delegado(a) quien lo presidirá |
| Subgerente de Planeación y Proyectos |
| Subgerente Jurídico |
| Subgerente corporativo |
| Subgerente de Servicios Operacionales e infraestructura |
| Jefe de la oficina de auditoría interna |
| Jefe de la Oficina Asesora de Comunicaciones |
| Director de Servicio al Transportador |
| Director de Servicio al Ciudadano |
| Director de Seguridad Operacional |
| Dirección de Infraestructura |
| Director de Gestión Humana |
| Director de Gestión Financiera |
| Director de Recursos Físicos y Negocios |
| Director de Recursos Tecnológicos |

Fuente. Resolución 115 de 11 set 2017 de la Terminal de Transporte S.A.

La Operación de la seguridad de la información estará a cargo del Oficial de Seguridad de la Información. El Director de Recursos Tecnológicos cumplirá los roles y responsabilidades en ausencia de este.

**Los Miembros del Comité de Sistema Integrado de Gestión tienen las siguientes responsabilidades relacionadas con la seguridad de la información:**

a. Revisar y aprobar las políticas de seguridad de la información de La Terminal de Transporte S.A.

b. Evaluar, revisar, aprobar y coordinar la implementación de los controles de seguridad de la información.

c. Garantizar la divulgación de las políticas y normas de seguridad de la Información a todos los empleados, proveedores y Clientes.

d. Coordinar revisiones independientes a las políticas de seguridad de la información, y la efectividad y eficiencia de los controles implementados.

e. Realizar reportes periódicos a la Gerencia de La Terminal de Transporte S.A. indicando el nivel de seguridad obtenido.

f. Apoyar el desarrollo de actividades de concientización y capacitación a todos los empleados que enfatice la importancia del cumplimiento de las políticas seguridad de la información y su contribución al logro de los objetivos del negocio.

COPIA CONTROLADA

g. El Comité SIG se reunirá semestralmente o cuando un incidente de seguridad requiera atención por parte del comité

**El Oficial de Seguridad de la información tiene las siguientes responsabilidades:**

a. Mantener actualizadas las políticas y normas de seguridad de la información de La Terminal de Transporte S.A. y los documentos asociados al SGSI.

b. Apoyar la identificación, evaluación y control de los riesgos de seguridad de la información de los diferentes procesos.

c. Verificar que los planes de tratamiento y controles definidos para mitigar los riesgos de seguridad de la información se ejecutan efectiva y eficientemente.

d. Desarrollar actividades de capacitación y concientización en temas relacionados con la seguridad de la información.

e. Apoyar la consolidación de la cultura de seguridad de la información entre todo el personal.

f. Coordinar el desarrollo de auditorías internas al SGSI.

g. Monitorear las violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada

h. Coordinar la implementación de acciones preventivas y correctivas del Sistema de Gestión de Seguridad de la Información con los respectivos responsables, de acuerdo con los resultados de las auditorías internas o externas.

i. Implementar y hacer seguimiento al plan de mejora continua del Sistema de Gestión de Seguridad de la Información.

j. Definir la estrategia de gestión de los riesgos de seguridad de la información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.

**Los empleados de La Terminal de Transporte S.A. tienen las siguientes responsabilidades:**

a. Conocer, respetar, cumplir y hacer cumplir las políticas y normas de seguridad de la información.

b. Proteger los activos de información a su cargo contra accesos físicos y lógicos no autorizados.

c. No divulgar, modificar, destruir o interferir información confidencial sin la autorización expresa del responsable de la información.

COPIA CONTROLADA

d. Reportar al Oficial de Seguridad de la información y/o comité SIG los eventos o incidentes de seguridad que sean detectados.

### 7.1.2. Segregación de tareas

a. Las tareas y responsabilidades que generen algún tipo de conflicto desde el punto de vista de seguridad de la información, deben ser segregadas para reducir el riesgo de modificación no autorizada o intencional de información.

b. Los directores de área, serán los encargados de verificar que exista segregación de las tareas y responsabilidades en cada una de sus áreas.

### 7.1.3. Contacto con autoridades

Los directores de área deben mantener una lista actualizada, visible y publicada de los contactos indispensables para mantener la operación de La Terminal de Transporte S.A.

### 7.1.4. Contacto con grupos de interés

El oficial de seguridad de la información debe mantener contacto permanente con foros de discusión de temas relacionados con la seguridad de la información y la gestión de incidentes.

### 7.1.5. Gestión de proyectos

a. La Seguridad de la información se debe tener en cuenta como medida prioritaria en la gestión de los proyectos de todas las áreas de la Organización.

b. La metodología de gestión de proyectos que asuma la Organización debe contemplar la seguridad de la información como uno de los principales ítems y se debe contemplar desde el inicio del proyecto en los que se incluya los mecanismos de intercambio seguro de información según sea el caso.

c. Se debe gestionar los riesgos de los proyectos relacionados a seguridad de la información como parte del seguimiento de esta actividad.

### 7.1.6. Normas de seguridad relacionadas con dispositivos móviles

a. El uso de dispositivos móviles (celulares, portátiles, tabletas, etc.) con información y/o aplicativos de La Terminal de Transporte debe ser autorizado por la Gerencia y estos deben ser protegidos mediante los siguientes controles:

- El almacenamiento de información clasificada como confidencial en los dispositivos móviles debe ser por y para uso exclusivo de las funciones del negocio.
- La conexión de los portátiles a una red de internet diferente a la de la Terminal de Transporte, debe

COPIA CONTROLADA

ser autorizada por el Director de Recursos Tecnológicos y el empleado a cargo del equipo debe contarcon herramienta de antivirus actualizada.

- Los empleados a cargo de los dispositivos móviles deben protegerlos de accesos físicos o lógicos no autorizados y no descuidarlos en lugares públicos.
- Se debe reportar de manera inmediata al Director de Recursos Tecnológicos la pérdida o daño del dispositivo móvil, con el fin de que se evalúen los riesgos asociados a la pérdida.

### 7.1.7. 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.

a. 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.

b. 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

c. 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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 la información.

COPIA CONTROLADA

## 8. SEGURIDAD DEL RECURSO HUMANO

### 8.1. PROCESO DE INGRESO

#### 8.1.1. Antes de la contratación

a. El proceso de selección de personal de La Terminal de Transporte S.A. se realizará de acuerdo con los procedimientos establecidos en la organización y estos deben dar cumplimiento a las leyes y regulaciones vigentes.

b. Antes de la contratación del personal seleccionado, se verificarán las referencias laborales, judiciales, comerciales y académicas, así como sus competencias y habilidades para garantizar que cumple con los requerimientos del perfil solicitado.

c. Los contratos laborales con empleados, contratistas y personal en misión deben indicar claramente sus responsabilidades para con la seguridad de la información de la Terminal de Transporte S.A.

#### 8.1.2. Durante el periodo de vinculación contractual con la Terminal de Transporte S.A.

a. Todos los trabajadores, sin importar el tipo de contrato, ya sea a término fijo o indefinido o contratistas por prestación de servicio, así como misionales, deben firmar un acuerdo de confidencialidad en el momento en que ingresan a La Terminal de Transporte S.A.

b. El acuerdo de confidencialidad con los empleados, debe estar vigente durante todo el tiempo de relación laboral con La Terminal de Transporte S.A

c. El acuerdo de confidencialidad que firman los empleados, debe establecer que toda la información a la cual tengan acceso es de propiedad de la Terminal de Trasporte, por lo cual, La Terminal de Transporte S.A se reserva el derecho para analizar y monitorear el uso que los empleados le den a esta información.

d. Las actividades de capacitación de seguridad de la información deben estar enfocadas en los requisitos de seguridad, el marco legal aplicable y el uso adecuado de los activos de información.

e. La Dirección de Gestión Humana debe coordinar que todos los empleados que ingresen a la Organización reciban una inducción que haga énfasis en las políticas y normas de seguridad de la información de La Terminal de Transporte S.A y el adecuado manejo que le deben dar a la información.

f. Todo el personal que cometa un fallo de seguridad, por ejemplo, la violación deliberada de estas políticas de seguridad de la información, incurrirá en falta disciplinaria para el caso de empleados de La Terminal de Transporte S.A o a través de contratos o procesos judiciales en caso de terceros.

g. Los procesos disciplinarios deben asegurar el tratamiento adecuado y justo de los empleados según lo establezca la Convención Colectiva de Trabajo y el Reglamento Interno del Trabajo.

COPIA CONTROLADA

h. Los periodos donde se disfruta vacaciones, días libres y otros contemplados en el reglamento interno de trabajo, así como los periodos asociados a incapacidades prologadas o permisos autorizados por eventos personales, deben ser informados de acuerdo con el tipo de contrato según su responsable: para contratos de planta y misionales Gestión Humana será el encargado de informar a Tecnología y para los contratos de contratistas el responsable será cada supervisor quien informe a Tecnología. En cualquiera de los casos, esta actividad debe ser realizada mediante la generación de un Ticket por cada responsable asignado para que Tecnología realice los respectivos ajustes o bloqueos temporales de los recursos y la reasignación de los permisos y accesos para quien los reemplace.

### 8.1.3. Cese o cambio de puestos de trabajo

a. Los empleados que se retiren de la Terminal de Transporte S.A deben recibir por parte del Subgerente y/o Director de Área un recordatorio acerca de los compromisos legales y éticos adquiridos con respecto a mantener la confidencialidad de la información a la cual tuvo acceso en el curso de su empleo.

b. Consideraciones similares deben ser aplicadas cuando un empleado de La Terminal de Transporte S.A cambie de funciones en una misma área o en áreas diferentes. En este caso, los directores involucrados en la transferencia del personal, deben garantizar que el acceso a la información confidencial de las áreas involucradas es protegido de accesos o modificaciones no autorizadas.

c. El acceso a la información, computadores, redes de datos e instalaciones físicas, deben ser revocadas de inmediato, cuando un empleado o un tercero se retira de La Terminal de Transporte S.A.

d. Previo a la finalización de las actividades establecidas en el contrato el colaborador independiente de su vinculación con la terminal (trabajador de planta, contratista o trabajador en misión) debe hacer entrega de los activos de información al jefe inmediato que le fueron asignados para su labor tanto físicos (documentos, pc, USB, entre otros) como en medios digitales. La información sensible que se manejó durante el periodo de vida laboral, deberá conservar su carácter de confidencialidad posterior a la finalización del contrato por un periodo de 5 años. De igual manera, como sucede en la relación contractual activa, se seguirá el mismo mecanismo para informar cualquier cambio al contrato por parte de los responsables mediante la generación de Ticket a Tecnología, para los bloqueos definitivos de los recursos y la reasignación de los permisos y accesos para quien los reemplace.

## 8.2. GESTIÓN DE ACTIVOS DE INFORMACIÓN

### Política para el manejo de la información

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.

COPIA CONTROLADA

### 8.2.1. Responsabilidad sobre los activos

#### 8.2.1.1. Inventario de activos de información

a. El oficial de seguridad de la información es quién lidera la gestión de los inventarios de los activos de información de la Terminal de Transporte S.A. por parte de cada área.

b. Cada una de las áreas de La Terminal de Transporte S.A debe llevar un inventario de los activos de información a su cargo.

c. Los datos mínimos según aplique que debe contener el inventario de los activos de información (físicos y digitales) son:

- Nombre
- Ubicación
- Serial
- Activo
- Responsable del activo
- Dueño del activo
- Clasificación del activo

d. El inventario de los activos de información debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:

- Cambios en el ambiente de negocios o estrategia empresarial (ingreso de nuevos clientes).
- Nuevas obligaciones legales, contractuales o reglamentarias.
- Pasado un año después de la última actualización del inventario.

#### 8.2.1.2. Propiedad de los activos

a. Los propietarios de los activos de información son responsables por la clasificación de sus activos y la definición y revisión periódica de las restricciones de acceso y demás controles aplicables para la protección de los mismos.

### 8.2.2. Clasificación de la información

a. Los propietarios o responsables de los activos de información en medio físico y/o digital deben realizar la clasificación de los mismos, de acuerdo con su valor, requerimientos legales vigentes, criterios de confidencialidad, sensibilidad, riesgo de pérdida o compromiso, requerimientos de retención y facilidad de recuperación que deben ser empleados.

b. Los requerimientos legales, contractuales, estatutarios y regulatorios deben ser considerados al momento de evaluar la clasificación de los activos de información.

c. Los niveles de confidencialidad en que se deben clasificar los activos de información son:

COPIA CONTROLADA

- Información de uso público o informativo (pública)
  Es la información administrada por la Terminal de Transporte S.A., que está a disposición del público en general, su divulgación no requiere de autorización especial dentro o fuera de la Terminal de Transporte S.A. y su función es de comunicación al personal en general.

  Algunos ejemplos de información pública son los siguientes: Catálogos de productos y servicios, información publicado en sitio Web, Declaración de Practicas de Certificados (DPC), etc.

- Información de uso interno o privada (privada)
  Información usada internamente en La Terminal de Transporte S.A. y que puede ser compartida con socios externos identificados (que pueden ser clientes o proveedores de servicios) sin cualquier daño material. La divulgación no autorizada de información privada, puede causar perjuicio importante a laTerminal de Transporte S.A.

  Algunos ejemplos de información privada son los siguientes: Información sobre nuevos productos, comunicados de marketing, otras informaciones de rutina que están relacionadas a la producción y distribución de productos, soporte a los sistemas de negocios, procedimientos internos, etc.

- Información de uso confidencial (confidencial)
  Información administrada por la Terminal de Transporte S.A., que debe ser conocida exclusivamente por un grupo autorizado de empleados de La Organización.

  El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del dueño y de acuerdos de confidencialidad. Así mismo, sudivulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

  Algunos ejemplos de información confidencial son los siguientes: Estrategias de gestión, datos de desempeño financiero, planes de lanzamientos, información crítica e importante de los trabajadores o de negocios.

### 8.2.3. Etiquetado de la información

a. La información debe ser etiquetada para su identificación ágil y garantizar su manipulación adecuada de acuerdo a lo descrito en el numeral 8.2.2.c niveles de confidencialidad.

b. Los correos electrónicos, deben contener en la parte inferior la siguiente leyenda:

*"Una empresa capaz de estructurar y operar soluciones de movilidad"*
*Antes de imprimir este correo piense bien si es necesario hacerlo. El ambiente es asunto de todos.*
*"La información aquí contenida es para uso exclusivo de la persona o entidad de destino. Está estrictamente prohibida su utilización, copia, descarga, distribución, modificación y/o reproducción total o parcial, sin el*

COPIA CONTROLADA

*permiso expreso de la Terminal de Transporte S.A, pues su contenido puede ser de carácter confidencial y/o contener material privilegiado. Si usted recibió esta información por error, por favor contacte en forma inmediata a quien la envió y borre este material de su computador. La Terminal de Transporte S.A. no es responsable por la información contenida en esta comunicación, el directo responsable es quien la firma o el autor de la misma."*

c. En el caso de que alguna presentación contenga información CONFIDENCIAL o de USO INTERNO, esta debe contener en la parte inferior de cada diapositiva, una etiqueta visible que identifique la clasificación asignada.

**8.2.4. Manejo de información**

a. La información de los clientes es clasificada como confidencial en toda la organización y su manejo debe estar limitado a actividades propias del negocio, no debe ser divulgada a personas no autorizadas.

b. La información clasificada como privada o confidencial debe cumplir con las siguientes normas:

- Los remitentes de información confidencial enviada a terceros, deben verificar que los destinatarios tienen el derecho de conocer la información antes del envío.
- El acceso a la información confidencial almacenada en las bases de datos y archivos digitales o archivosfísicos, debe ser estrictamente controlado y debe otorgarse por parte de los dueños o responsables dela información de acuerdo a condiciones exclusivas del negocio.
- No descuide la información confidencial, evite ubicar esta información en lugares de fácil acceso por externos, como zonas con tránsito público como e-commerce, clientes, contratistas o proveedores. Esta información debe tener controles que dificulten el acceso no autorizado. Por medio de cajoneras,archivos, bloqueo de equipo desatendido.
- No hable en sitios públicos sobre información interna. Ejemplo: ascensores, restaurantes, buses
- En lo posible, la Información confidencial deber tratarse en recintos cerrados, tales como salas.
- Destruya de forma segura toda la información confidencial, cuando deje de ser necesaria.

**8.2.5. Manejo de medios de almacenamiento**

a. El uso de medios de almacenamiento removibles como memorias USB, discos externos, DVD, discos ópticos, etc. en los equipos en donde se procesa o almacena información confidencial debe ser autorizado por la Gerencia de la Terminal de Trasporte S.A. o quien ella delegue y deben ser de uso exclusivo para actividades del negocio.

b. Todos los medios de almacenamiento removibles en donde exista información clasificada como confidencial (físicos y digitales) deben ser guardados en áreas físicamente controladas y no deben ser desatendidos.

c. La salida de un medio de almacenamiento que contenga información confidencial debe ser autorizada por el propietario de la información.

COPIA CONTROLADA

d. La información electrónica o digital que ya no es necesario almacenar en un medio removible, debe ser eliminada utilizando métodos que impidan su recuperación.

e. La información física que no sea necesario almacenar, debe ser destruida antes de enviar a la basura.

f. Los papeles que contienen información confidencial o privada no se pueden utilizar como papel reciclable.

g. Cuando se almacena en una misma ubicación física o electrónica información de diferentes niveles de confidencialidad, los controles que se implementen deben proteger la información más sensible y se debe garantizar el máximo nivel de control de acceso.

## 8.3. GESTIÓN DE CONTROL DE ACCESOS LÓGICOS

### 8.3.1. Requisitos del negocio para el control de acceso lógico a la información:

#### 8.3.1.1. Política de control de acceso

a. 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.

#### 8.3.1.2. Acceso a redes y servicios de red

a. 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.

b. Los sistemas de autenticación y autorización para los servidores de red y aplicativos deben estar conformados por un usuario y una contraseña.

c. 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.

### 8.3.2. Gestión de acceso de usuarios:

#### 8.3.2.1. Registro y cancelación de usuarios

a. 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:

i. La autorización por parte del dueño de la información para obtener acceso a los diferentes sistemas de

COPIA CONTROLADA

información.

ii. 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.

b. 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.

c. El Director de Gestión Humana 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.

d. El Director de Gestión Humana 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, de acuerdo a los lineamientos estipulados en el numeral 7.1.2 del presente documento.

e. 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.

f. 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.

g. 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 a la matriz de roles y perfiles.

h. 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.

#### 8.3.2.2. Suministro de acceso de usuarios

a. 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.

b. 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

#### 8.3.2.3. Gestión de derechos de acceso privilegiado

a. 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

COPIA CONTROLADA

sus actividades y responsabilidades.

b. 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.

c. Las actividades de los usuarios con perfiles de administración deben ser registradas en un log de auditoria.

d. 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.

e. 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.

f. 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.

g. El acceso a los datos almacenados en las bases de datos, se debe realizar exclusivamente por los aplicativos.

h. 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.

**8.3.2.4. Gestión de la información de autenticación secreta de usuarios:**

a. 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.

b. Lo repositorios que contienen la información de usuarios y contraseñas de los aplicativos y sistemas operativos debe ser cifrados.

c. El transporte por la red de la información de usuarios y contraseñas se debe realizar por medio de mecanismos de cifrado de información.

COPIA CONTROLADA

**8.3.2.5. Revisión de los derechos de acceso de los usuarios:**

Cada dueño o responsable de información debe revisar cada seis meses la matriz de roles y perfiles con el fin de verificar los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan.

**8.3.2.6. Retiro o ajuste de los derechos de acceso:**

Con base en la revisión semestral, los dueños o responsable de información deben retirar o ajustar los permisos, garantizando el cumplimiento del principio de menor privilegio.

**8.3.3. Control de acceso a sistemas y aplicaciones:**

**8.3.3.1. Restricción de acceso a la información**

El acceso a la información clasificada como confidencial debe ser otorgada por los dueños de la información única y exclusivamente a los funcionarios que deben tener acceso para desarrollar sus actividades y responsabilidades y dando cumplimiento a las políticas de control de acceso lógico.

**8.3.3.2. Procedimiento de acceso seguro**

a. El acceso a los aplicativos y sistemas de información de la Terminal de Transporte debe estar controlado por medio de mecanismos de autenticación y autorización.

b. Los sistemas de autenticación y autorización para los aplicativos y sistemas de información deben estar conformados por un usuario y una contraseña.

c. Los privilegios de acceso de los usuarios a los aplicativos 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.

**8.3.3.3. Gestión de contraseñas**

a. Las contraseñas de todos los aplicativos con los que cuente la Terminal deben cumplir con las siguientes características:

- Longitud mínima de 8 caracteres
- Ser alfanumérica
- Debe contener mayúsculas y minúsculas y caracteres especiales

b. La contraseña debe expirar cada 60 días y debe ser cambiada de manera obligatoria para todos los usuarios.

c. Si el aplicativo no informa el cambio de la contraseña, los usuarios tienen la responsabilidad de cambiar

COPIA CONTROLADA

su contraseña cada 60 días.

d. Los usuarios deben cambiar la contraseña en el primer inicio de sesión.

#### 8.3.3.4. Programas utilitarios privilegiados

El uso de programas de diagnóstico de la red, scanner, cracking de contraseñas, etc. debe ser restringidoy usado exclusivamente por los funcionarios de la dirección de recursos tecnológicos.

#### 8.3.3.5. Control de acceso a código fuente

a. El director de recursos tecnológicos debe garantizar que el acceso al código fuente de los aplicativos desarrollados al interior de La Terminal de Transporte, o adquiridos a terceros está controlado y asignado exclusivamente a los funcionarios que lo requieren para el desarrollo de sus responsabilidades.

## 8.4. POLITICA SOBRE CONTROLES CRIPTOGRÁFICOS

### 8.4.1. Gestión de llaves criptográficas

a. Los usuarios finales deben dar el uso, protección adecuada y aplicar los controles necesarios para evitar accesos no autorizados a las llaves criptográficas asignadas.

b. Se debe distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

c. 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.

## 8.5. GESTIÓN DE SEGURIDAD FÍSICA Y AMBIENTAL

### 8.5.1. Áreas Seguras:

a. Las áreas seguras son aquellas que necesitan autorización previa para permitir el ingreso de personas ajenas al área, por la naturaleza de la información confidencial que se maneja o los procesos que allí se realizan. En La Terminal de Transporte S.A., se identificaron las siguientes áreas seguras:

- Centro de cómputo principal
- Área de Tecnología
- Áreas de archivo activo e inactivo.
- Área de archivo de hojas de vida del personal.
- Sub centros de cableado estructurado
- Sub centro de Circuito cerrado de televisión CCTV

Todas estas áreas deben estar debidamente marcadas como zonas restringidas y se debe registrar el acceso

COPIA CONTROLADA

a las mismas.

**8.5.1.1. Perímetro de seguridad física:**

Las áreas seguras deben estar delimitadas físicamente y el acceso físico debe ser controlado.

**8.5.1.2. Controles físicos de entrada:**

Las áreas seguras deben contar con mecanismos para controlar el acceso físico.

**8.5.1.3. Protección contra amenazas externas y ambientales:**

a. Las áreas seguras de la Terminal de Transporte S.A. deben tener medidas de protección para reducir al mínimo la posibilidad y las repercusiones de incidentes como incendios, inundaciones, terremotos, desastres naturales, explosiones, disturbios civiles o sabotajes.

b. El centro de cómputo debe contar con un sistema de UPS, sistema de control de temperatura, así como de condiciones eléctricas acordes a las normas internacionales.

c. Todas las estaciones de trabajo deben estar soportadas por un sistema de planta eléctrica

d. Los operadores, administradores y visitantes frecuentes a las áreas seguras, deben ser capacitados en los procedimientos que deben seguir cuando se presente un evento de origen físico que afecte la continuidad en la operación normal del área.

e. Se debe establecer y ejecutar un plan de mantenimientos preventivos que cobije todos los recursos informáticos y de soporte ambiental de las áreas seguras de La Terminal de Transporte S.A.

f. En los centros de cómputo no se deben tener materiales inflamables.

**8.5.1.4. Trabajo en áreas seguras:**

a. El ingreso de personal ajeno a las áreas seguras debe ser autorizado por el director del área correspondiente.

b. Una vez autorizado el ingreso del visitante, el empleado visitado deberá recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área segura.

c. Para todos los visitantes a las áreas seguras, se registrará la fecha y hora de ingreso, empleado a quien visita y fecha y hora de la salida. El registro de esta información se puede hacer electrónico o en minutas manuales.

d. El ingreso de dispositivos de grabación de audio, fotos y video a las áreas de acceso restringido debe

COPIA CONTROLADA

ser autorizado por el Director del área segura.

### 8.5.2. Seguridad de los equipos

#### 8.5.2.1. Ubicación de sistemas críticos

a. Los equipos de misión crítica y los que procesan o almacenan información confidencial como servidores, equipos de comunicaciones, equipos de protección ambiental, deben estar ubicados en el centro de cómputo de La Terminal de Transporte S.A.

b. Está prohibido comer, fumar o beber en el centro de cómputo o instalaciones con equipos tecnológicos

#### 8.5.2.2. Equipos de respaldo

a. Los centros de cómputo deben contar con sistemas de respaldo eléctrico (UPS y planta eléctrica) que proteja los equipos de misión crítica.

b. Las condiciones ambientales de los centros de cómputo deben estar protegidas por sistemas de aires acondicionados que cumplan con las especificaciones necesarias para las áreas del centro de cómputo.

c. Las condiciones eléctricas y ambientales como temperatura y humedad deben ser controladas en los centros de cómputo o áreas en donde se ubiquen equipos de misión crítica.

#### 8.5.2.3. Seguridad en el cableado

**Política de Instalación de Cableado**

La Instalación de Cableado Estructurado: Planeación, diseño, construcción, instalación, administración y mantenimiento del cableado estructurado de telecomunicaciones de la Terminal es responsabilidad del proceso Fortalecimiento de Tecnología e Información, debe cumplir con las normas técnicas o estándares adoptados por el mismo, con el fin de garantizar la integridad, conservar la estética y la seguridad de las redes

a. Los sistemas de cableado estructurado de las diferentes instalaciones de La Terminal de Transporte S.A. deben cumplir con el estándar internacional TIA/EIA-568-B como mínimo.

b. Los cables de datos se deben instalar por canaletas que impidan ataques de interceptación o daño.

c. Los cables que transportan datos debes estar físicamente separados de los cables de energía eléctrica para evitar interferencias.

d. Los cables deben ser claramente identificados y marcados en toda su trayectoria.

COPIA CONTROLADA

e. Los planos de cableado estructurado y eléctrico deben estar actualizados y disponibles para el personal autorizado en su manejo.

**8.5.2.4. Mantenimiento de los equipos:**

a. Los equipos en donde se procesa información sensible o critica para el normal funcionamiento de La Terminal de Transporte S.A., deben contar con planes de mantenimientos preventivos y correctivos que garanticen su disponibilidad e integridad.

b. Se debe establecer un plan de mantenimiento preventivo en periodos de tiempo acordes a las recomendaciones y especificaciones del proveedor.

c. Exclusivamente el personal autorizado del mantenimiento puede realizar reparaciones y su trabajo debe ser documentado. Si el equipo debe ser retirado de las instalaciones para realizar las reparaciones, la confidencialidad e integridad de cualquier información debe ser garantizada.

**8.5.2.5. Salida de activos:**

a. En caso de retiro de un equipo de las instalaciones de La Terminal de Transporte S.A., debe diligenciarse el formato **FTI-FT25 Autorización salida de activos**.

b. En caso de presentarse un daño sobre algún elemento de trabajo por causas como: golpes, derrame de bebidas o elementos extraños, la reparación o reposición estará a cargo de la persona que retiro el equipo.

**8.5.2.6. Seguridad de los equipos y activos fuera de las instalaciones de La Terminal de TransporteS.A.:**

a. Todo equipo de propiedad de La Terminal de Transporte S.A., que por razones del servicio esté fuera de las instalaciones de la organización, no debe ser desatendido en lugares públicos por su responsable.

b. La Terminal de Transporte S.A. debe asegurar a través de pólizas de seguro las computadoras portátiles.

c. En los PC de escritorio, Tablet o portátiles que por razones del servicio salen de la Organización no se debe almacenar información clasificada como confidencial.

**8.5.2.7. Reutilización o retirada segura de dispositivos de almacenamiento:**

a. Toda la información almacenada en computadores que se van a dar de baja ya sea por obsolescencia, daño o no uso, debe ser eliminada utilizando técnicas de borrado seguro que garanticen que la información original no sea recuperable.

**8.5.2.8. Equipos desatendidos:**

a. 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

COPIA CONTROLADA

protector de pantalla.

La opción de protector de pantalla de Windows debe configurarse con los siguientes parámetros:

- Activar el protector de pantalla después de cinco minutos de inactividad del computador.
- El desbloqueo requiere contraseña de red.
- Toda estación de trabajo, debe tener configurado el papel tapiz empresarial definido.

**8.5.2.9. Política de puesto de trabajo despejado:**

a. Los empleados, clientes, proveedores o consultores externos deben garantizar que la información clasificada confidencial que no esté siendo utilizada por personal autorizado, debe permanecer siempre bajo llave y no debe ser desatendida en ninguna ubicación no controlada.

b. 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.

## 8.6. SEGURIDAD EN LAS APLICACIONES

### 8.6.1. Responsabilidades y procedimientos de operación:

#### 8.6.1.1. Documentación de procedimientos de operación:

- La Dirección de Recursos Tecnológicos debe documentar los procedimientos de administración y operación de la infraestructura tecnológica de La Terminal de Transporte S.A.

- Los procedimientos documentados son:

  - Backup y recuperación de información
  - Gestión de cambios
  - Gestión de incidentes
  - Gestión de usuarios, roles y perfiles de seguridad
  - Mantenimiento preventivo y correctivo TI
  - Administración de redes y comunicaciones
  - Configuración, administración y uso del directorio activo
  - Antivirus

#### 8.6.1.2. Gestión de cambios:

a. La Dirección de Recursos Tecnológicos debe establecer un procedimiento formal y documentado para controlar todos los cambios de hardware y/o software de la infraestructura de TI.

COPIA CONTROLADA

b. Los procedimientos de control de cambios de la infraestructura deben asegurar que:

- Los cambios significativos se identifican y se documentan.
- Los planes del cambio se establecen y se prueban.
- Los impactos potenciales de los cambios se identifican y se analizan, incluyendo los impactos a nivel deconfidencialidad, integridad o disponibilidad de la información
- Se obtiene la aprobación formal para los cambios significativos por parte del equipo evaluador decambios en TI Los detalles del cambio se comunican a todas las áreas involucradas.
- Se documentan las actividades de roll back para abortar y recuperarse de cambios fallidos.
- Todos los cambios son probados en ambientes controlados por los dueños de la información antes desubir a los ambientes de producción.

c. Los cambios que se realicen sobre los recursos de TI de misión crítica deben ser registrados en el formato de control de cambios.

d. Antes de realizar un cambio de hardware y/o software en los recursos de TI de misión crítica, se debe hacer una copia de respaldo de la información.

e. El procedimiento de control de cambios debe contemplar cambios de emergencia.

**8.6.1.3. Gestión de capacidades:**

a. La Dirección de Recursos Tecnológicos debe realizar una revisión periódica de las necesidades de capacidad de los recursos de TI, con el fin de identificar el nivel de desempeño ofrecido y las necesidades de crecimiento requeridas para satisfacer los requerimientos de La Terminal de Transporte S.A.

b. Los recursos de TI que se deben monitorear permanentemente son:

- Nivel de almacenamiento de los servidores de base de datos de los aplicativos críticos y misionales.
- Nivel de Tráfico en la red
- Niveles de utilización de procesamiento y memoria de los servidores de los aplicativos críticos y misionales.

**8.6.1.4. Separación de entornos de desarrollo, pruebas y producción:**

a. La Dirección de Recursos Tecnológicos debe asegurar que los ambientes de desarrollo de software, pruebas y producción se encuentran en ambientes lógicamente separados y con controles de acceso independientes.

b. La Dirección de Recursos Tecnológicos debe establecer un procedimiento formal y documentado para la transferencia de software entre los ambientes de desarrollo, pruebas y producción.

COPIA CONTROLADA

c. El ambiente de pruebas o calidad debe emular el ambiente de producción tanto como sea posible.

d. La información confidencial que sea necesario trasladar a los ambientes de desarrollo debe ser enmascarada antes de pasarla a desarrollo.

**8.6.2. Protección contra código malicioso:**

a. La Dirección de Recursos Tecnológicos debe garantizar que todos los computadores conectados en la red de La Terminal de Transporte S.A. tienen instalado el software antivirus de acuerdo con el estándar vigente.

b. Se deben implantar los mecanismos de actualización permanente y en línea del software antivirus instalado en los computadores conectados en la red. De igual forma, se debe garantizar un mecanismo semiautomático o manual que permita la actualización del antivirus instalado en computadores que no se conectan de manera permanente a la red.

c. Quincenalmente se debe revisar la consola de administración del software antivirus, con el fin de identificar los computadores que no tienen la última versión instalada. De ser necesario, se aplicará un procedimiento manual de actualización por parte de la Dirección de Recursos Tecnológicos.

d. El software antivirus debe ser configurado para el escaneo en línea de todas las unidades de almacenamiento.

e. Todo CD, memoria USB o disco externo que sea conectado en un computador de la Terminal de Transporte S.A. independientemente de su procedencia, debe ser escaneado con el software antivirus antes de ser utilizado.

f. Los usuarios deben reportar de inmediato al área de soporte cualquier comportamiento anormal del computador o indicio de la presencia de virus, con el fin de prevenir la propagación del mismo.

**8.6.3. Copias de seguridad:**

**Política de Copias de Respaldo**

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

COPIA CONTROLADA

usados, custodiados o producidos por esto, deben tener en cuenta que esta información se debe alojar en la carpeta MIS DOCUMENTOS.

a. Los dueños de la información deben garantizar que se realiza Backup a toda la información sensible almacenada en los servidores de red.

b. 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.

c. 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 continuidaddel negocio).
- Periodo de retención.

d. 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.

e. Trimestralmente, se deben realizar pruebas de restauración de un Backup para verificar el contenido y la usabilidad del mismo.

**8.6.4. Registro y seguimiento:**

**8.6.4.1. Registro de eventos:**

a. Los sistemas de información que procesan y/o almacenan información crítica y sensible para la operación del negocio e información confidencial deben registrar las actividades de los usuarios en registros de auditoría. Los registros de auditoría deben incluir:

- Identificación de los usuarios
- Fecha y hora eventos
- Identificación o dirección IP del computador desde el que se hace la conexión.
- Intentos fallidos de conexión
- Cambios de configuración del sistema
- Uso de utilidades del sistema
- Archivos usados y tipo de interacción
- Operaciones privilegiadas
- Intentos de acceso no autorizado
- Cambios o intento de cambios a los parámetros de seguridad de los sistemas de información
- El registro de auditoría debe ser revisados periódicamente

COPIA CONTROLADA

**8.6.4.2. Protección de la información de Registro de eventos:**

a. El acceso a los registros de auditoría debe estar restringidos al Director de Recursos Tecnológicos (Oficial de seguridad de la información), Auditoría Interna y administradores de los sistemas de información.

b. Se deben realizar copias de respaldo a los registros de eventos de auditoría.

**8.6.4.3. Protección de la información de Registro de eventos**

a. Todas las actividades realizadas por los usuarios con privilegios de administración y operación sobre los sistemas de información deben ser registradas en logs de auditoría. Estos logs deben incluir:

- Identificación del usuario administrador y/u operador
- Fecha y hora del evento
- Información del evento

b. Las fallas y los errores de los sistemas de información se deben registrar y analizar para determinar el plan de acción apropiado.

**8.6.4.4. Sincronización de relojes**

Los relojes de los diferentes sistemas de información deben estar sincronizados con la hora legal de Colombia definida por el Instituto Nacional de Metrología.

**8.6.5. Control de sistemas operativos**

a. La instalación, configuración y actualización de los sistemas operativos estará a cargo de la dirección de recursos tecnológicos

**8.6.6. Gestión de las vulnerabilidades técnicas**

a. La Dirección de Recursos Tecnológicos, debe coordinar la realización cada doce meses de una prueba de ethical hacking y análisis de vulnerabilidades en los equipos que soportan los aplicativos críticos y misionales.

b. Se debe desarrollar un plan de tratamiento para mitigar los riesgos identificados en las pruebas de ethical hacking.

c. La instalación y uso de software especializado para identificación de vulnerabilidades técnicas sobre la red y los aplicativos de La Terminal de Transporte debe estar restringido y exclusivo para los funcionarios de la dirección de recursos tecnológicos.

COPIA CONTROLADA

**8.6.7. Controles de auditoría de información**

a. Los requerimientos y actividades de los procesos de auditorías a los sistemas operativos y sistemas de información deben ser planeados y los permisos a los auditores asignados con privilegios exclusivamente de lectura sobre la información.

## 8.7. SEGURIDAD EN LAS TELECOMUNICACIONES

### 8.7.1. Gestión de la seguridad en las redes

#### 8.7.1.1. Controles de redes

a. Los procedimientos de administración y operación de las redes de comunicaciones deben estar debidamente documentados y protegidos contra acceso no autorizado.

b. Los puntos de conexión física a la red cableada que no estén siendo utilizados se deben desconectar.

c. La dirección de recursos tecnológicos debe monitorear la disponibilidad de las redes de comunicaciones.

d. La Dirección de Recursos Tecnológicos debe establecer los acuerdos de nivel de servicios necesarios en los enlaces de comunicaciones para la correcta operación, adicionalmente, debe coordinar con los proveedores externos la implementación de estos niveles de servicio.

#### 8.7.1.2. Seguridad en los servicios de red

#### 8.7.1.3. Normas en el uso de internet

a. El acceso a internet debe ser aprobado por el jefe inmediato.

b. El acceso a internet está restringido únicamente a páginas de información financiera, técnica, comercial, cultural, a las cuales por desarrollo de las actividades propias de cada cargo sea necesario ingresar.

c. El acceso a internet NO puede ser utilizado para los siguientes propósitos:

- Actividades relacionadas a juegos online por internet
- Ingreso a cualquier material considerado como pornográfico, ofensivo, discriminatorio o ilegal según las normas internas de La Terminal de Transporte S.A. y la legislación vigente
- Descargar música, videos, fotos, fondos de pantalla, programas, juegos etc., los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor.
- Los servicios de RADIO y TV por demanda deben ser autorizados por el jefe inmediato.
- Utilizar los servicios de Internet para enviar archivos que sean confidenciales y de propiedad exclusiva

COPIA CONTROLADA

de la Terminal de Transporte S.A.

- Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocios particulares.
- Utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegido por las leyes vigentes. Esto incluye todos los archivos protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.
- El acceso no autorizado a cualquier intento de prueba, verificación o rastreo (scan) de vulnerabilidades de un sistema o red, violando las medidas de seguridad o de autenticación sin la expresa autorización del propietario del sistema o la red.
- El acceso a redes sociales debe ser autorizado por el jefe inmediato.

**8.7.1.4. Normas de uso del correo electrónico**

a. El servicio de correo electrónico es para uso exclusivo de las actividades relacionadas con el trabajo de cada empleado.

b. El envío de información clasificada como confidencial, debe ser aprobado por los dueños de la información y/o Gerencia.

c. Se prohíbe la difusión no solicitada de puntos de vista personales referentes a temas políticos, raciales y religiosos, al igual que la inclusión de mensajes sobre creencias, frases célebres, convocatorias políticas entre otros, al igual que usar el email para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

d. Se prohíbe fomentar el envío de cadenas de mensajes, recepción o envío de mensajes con archivos adjuntos con extensiones .exe, .avi, .mp3, mp4, .vbs, .mpg, .Jpg.

e. Este servicio no debe usarse para enviar SPAM o mensajes no solicitados ni tampoco para enviar material obsceno e ilegal o relacionado a pornografía.

f. Está prohibido configurar reglas en los buzones de correo electrónico que reenvíen los mensajes a servidores públicos de internet como Hotmail, Yahoo, El reenvío de mensajes a dominios privados debe ser autorizado por el jefe inmediato.

g. No se puede utilizar el correo electrónico, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de La Terminal de Transporte S.A.

h. No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye sin limitación alguna, todo material protegido por derechos de autor (copyright), marcas registradas, secretos comerciales u otros de propiedad intelectual.

i. El tamaño de los archivos adjuntos está asociado al perfil de usuario creado.

COPIA CONTROLADA

j. La firma será la que se defina desde la Oficina Asesora de Comunicaciones y de acuerdo con las disposiciones establecidas.

k. Está prohibido adjuntar firmas escaneadas.

l. En caso de recibir un mensaje bajo sospecha de virus, (de personas desconocidas con asuntos desconocidos o sospechosos) no se debe abrir y se debe reportar de inmediato a la Dirección de Recursos Tecnológicos.

**8.7.1.5. Separación en la red.**

a. Las redes de comunicaciones en las cuales están conectados los servidores de misión crítica deben estar separadas de las redes de usuarios finales.

b. Las redes inalámbricas para clientes no deben permitir el acceso a las redes de los servidores de misión critica

**8.7.2. Transferencia de información:**

**8.7.2.1. Políticas y procedimientos de transferencia de información**

a. El Director de Recursos Tecnológicos (Oficial de Seguridad de la información) debe documentar los procedimientos y controles para el intercambio de información utilizando medios digitales. Los controles que se deben tener en cuenta son:

- Se debe proteger la información confidencial contra intercepción, copia, modificación o destrucción.
- 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

b. La Dirección de Recursos Tecnológicos debe controlar los riesgos relacionados con el envío de información confidencial por medio de las conexiones inalámbricas.

**8.7.2.2. Acuerdos sobre trasferencia de información**

a. Los empleados que requieran enviar y/o recibir información de un tercero, deben establecer un acuerdo

COPIA CONTROLADA

de intercambio en el que se deben tener en cuenta:

i. 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 eldueño de la información.
- Se deben definir claramente los responsables del envío, recepción y notificación del intercambio deinformación.
- Se deben definir los acuerdos de retención de dicha información.
- Establecer las responsabilidades de derechos de autor y licenciamiento

## 8.8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

### 8.8.1. Requisitos de seguridad de los sistemas de información:

#### 8.8.1.1. Análisis y especificación de los requisitos de seguridad

a. Los requerimientos de seguridad que deben cumplir los nuevos desarrollos de software o productos de software adquiridos por La Terminal de Transporte S.A. deben ser definidos por los dueños de la información y el Director de Recursos Tecnológicos (oficial de seguridad de la información) y deben contemplar las buenas prácticas de desarrollo. Esta definición se debe realizar antes de iniciar el proceso de desarrollo o adquisición del software.

b. Todos los productos de software adquiridos o desarrollados internamente deben ser probados antes de ser puestos en producción, con el fin de garantizar el cumplimiento de los requerimientos de seguridad definidos.

c. Todos los proyectos de desarrollo o adquisición de software deben contar con un análisis de riesgo para documentar los requerimientos de control necesarios.

#### 8.8.1.2. Seguridad de las comunicaciones en servicios accesibles por redes publicas

Los servicios de La Terminal de Transporte S.A. accesibles por terceros a través de redes públicas o redes privadas deben ser protegidos en todos los casos por canales cifrados utilizando técnicas como redes privadas virtuales (VPN) y/o certificados digitales para páginas seguras utilizando protocolos como SSL.

#### 8.8.1.3. Desarrollo contratado externamente

a. Es responsabilidad de la Dirección de Recursos Tecnológicos **supervisar** el aseguramiento de la calidady de producción de los desarrollos hechos por los contratistas.

b. El nuevo software garantizará la confidencialidad, integridad y disponibilidad de los demás sistemas de información, aplicaciones, programas con los que cuente la Terminal de Transporte S.A.

COPIA CONTROLADA

c. La Dirección de Recursos Tecnológicos **podrá** verificar el avance del desarrollo, acorde con lascondiciones pactadas en el contrato que La Terminal de Transporte S.A y el contratista hayan suscrito.

Es necesario que el software desarrollado por contratistas cumpla con los siguientes requerimientos:

- El software adquirido contará con licenciamiento que incluya actualización de versiones, de tal forma que permita que la plataforma tecnológica esté siempre en las últimas versiones de software que salgan al mercado y así evitar tener software obsoleto.

- Los contratos con terceros para el desarrollo y adquisición de software contarán con el mantenimiento, soporte y horas de desarrollo de nuevas funcionalidades para evitar su obsolescencia y se debe garantizar que durante la instalación del mismo no afecte la seguridaddel software del sistema.

- Existan políticas de soporte, mantenimiento y desarrollo de nuevas funcionalidades de acuerdocon la normativa vigente y las necesidades de los usuarios de tal forma que permita manteneractualizado dicho software.

**8.8.1.4. Pruebas de los sistemas y paso a producción**

a. Es de vital importancia que el área que realiza el requerimiento de modificaciones o nuevas funcionabilidades del software realice las pruebas de los sistemas de información, con el fin de garantizar la funcionalidad de estos y verificar que los cambios realizados cumplen con el requerimiento.

b. Con la finalidad de minimizar los riegos que puedan afectar la disponibilidad de la información se deben realizan pruebas que permitan validar:

- La compatibilidad, el funcionamiento adecuado y continúo del software desarrollado en diferentes plataformas: hardware, sistemas operativos, redes.
- La integración, comprobando las conexiones y comunicaciones entre los diferentes módulos del software desarrollado.
- La función, probando si permite asegurar que el sistema cumple con la funcionalidad para el cual fue hecho, y cumple con las especificaciones técnicas esperadas.
- El desempeño con la finalidad de establecer la eficiencia del sistema, estableciendo posibles fallas antes de su puesta en marcha.
- La instalación, la cual consiste en instalar el sistema de información en el servidor que alojará la base de datos o los archivos fuente de éste.

c. Datos de prueba: La Dirección de Recursos Tecnológicos deberá proteger los datos de prueba, de tal forma que no se revele información confidencial de los ambientes de producción.

COPIA CONTROLADA

d. Es necesario dejar documentado el resultado de las pruebas realizadas al sistema de información.

e. El paso a producción debe incluir:

- Aprobación del dueño del proceso
- Aprobación del usuario solicitante
- Aprobación del Director de recursos Tecnológicos
- Actualización de la documentación del aplicativo

## 8.9. SEGURIDAD EN LAS RELACIONES CON TERCEROS

### 8.9.1. Relaciones con los proveedores

#### 8.9.1.1. Seguridad de la información en la relación con proveedores

a. Todos los proveedores que tengan acceso a la red o información de La Terminal de Transporte deben cumplir y acatar las políticas de seguridad de la Información.

b. Los directores de área deben informar y capacitar a todos los proveedores y sus empleados acerca del cumplimiento de las políticas de seguridad de la información.

#### 8.9.1.2. Tratamiento de la seguridad en los acuerdos con proveedores

a. Todos los contratistas de servicios externos de La Terminal de Transporte S.A. deben firmar un acuerdo de confidencialidad de la información a la cual tengan acceso en el desarrollo de las actividades contratadas.

b. El acuerdo de confidencialidad con terceros, debe estar vigente durante todo el tiempo de relación comercial o laboral con el contratista de servicios externos.

c. El acuerdo de confidencialidad con los contratistas de servicios externos debe establecer que toda la información a la cual tengan acceso es de propiedad de La Terminal de Transporte S.A., por lo cual la Compañía se reserva el derecho para analizar y monitorear el uso que los contratistas de servicios externos le den a esta información.

d. Todas las conexiones entre La Terminal de Transporte S.A. y las entidades externas se debe limitar a los equipos y aplicaciones específicas que se deben trabajar. No se debe permitir el acceso ilimitado a las redes y sistemas de información de La Terminal de Transporte S.A. a personal de terceros.

e. Una vez el contratista de servicios externos haya culminado sus actividades comerciales con La Terminal de Transporte S.A., debe retornar y/o destruir toda la información confidencial almacenada en sus equipos en el desarrollo de las actividades.

COPIA CONTROLADA

### 8.9.2. Gestión de la presentación de servicios de proveedores

#### 8.9.2.1. Seguimiento y revisión de los servicios de los proveedores

a. Los directores de área deben hacer seguimiento de la entrega de los servicios de terceros.

b. Se deben realizar revisiones y auditorías periódicas sobre responsabilidades contractuales entre el contratista y la Entidad.

c. Los proveedores deben generar periódicamente informes de gestión acerca del cumplimiento de sus servicios y los planes de acción cuando los acuerdos de servicio no se cumplen totalmente.

#### 8.9.2.2. Gestión de cambios en los servicios de los proveedores

a. Los cambios en los objetivos, alcances y/o niveles de servicios ofrecidos en los servicios con los proveedores deben ser controlados mediante un procedimiento formal de gestión de cambios.

## 8.10. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

### 8.10.1. Responsabilidades y procedimientos:

a. El Director de Recursos Tecnológicos (Oficial de Seguridad de la información) de la Terminal de Transporte S.A. es responsable del registro, documentación, seguimiento y comunicación de los resultados de la gestión a los incidentes de seguridad presentados.

b. La Dirección de Recursos Tecnológicos da respuesta ante los incidentes de seguridad de la información. Es responsable de:

- Análisis técnico de los incidentes presentados
- Coordinar los refuerzos técnicos
- Coordinar el apoyo de consultores externos si es necesario.
- Coordinar y adelantar las actividades para la consecución del presupuesto requerido para la solucióndel incidente si lo amerita.
- Determinar el momento apropiado para reportar al comité SIG el plan de continuidad del negocio.
- Comunicar a la Gerencia general la información relacionada con la gestión de los incidentes de seguridad de la información.

c. El procedimiento de gestión de incidentes debe incluir los siguientes aspectos: detección, análisis, contención, erradicación y recuperación del incidente.

### 8.10.2. Notificación de los eventos de seguridad de la información:

a. El Director de Recursos tecnológicos debe implementar, documentar e informar a todos los empleados

COPIA CONTROLADA

y consultores externos un procedimiento para el reporte y escalamiento de incidentes de seguridad de la información.

b. Los procedimientos de reporte y escalamiento de incidentes, deben identificar claramente los puntos de contacto y los responsables de solución y seguimiento de los incidentes de seguridad.

**8.10.3. Notificación de puntos débiles de seguridad:**

a. Todos los empleados, clientes, proveedores y consultores externos deben informar al Director de Recursos Tecnológicos (Oficial de Seguridad de la información) de La Terminal de Transporte S.A. cualquier debilidad observada o sospecha de un incidente de seguridad de la información.

b. El Oficial de Seguridad de la información debe registrar el reporte de todos los incidentes de seguridad y las acciones tomadas para su solución.

Aprendizaje de los incidentes de seguridad de la información:

a. El Director de Recursos Tecnológicos (Oficial de Seguridad de la información) debe mantener una base de datos de conocimiento, la cual debe contener toda la información relacionada con los incidentes de seguridad presentados y su respectiva solución.

b. La base de datos de conocimiento de incidentes de seguridad debe ser protegida contra acceso no autorizado

**8.10.4. Recopilación de evidencias:**

a. El Director de Recursos Tecnológicos (Oficial de Seguridad de la información) debe garantizar que todos los archivos electrónicos o físicos recopilados como evidencia en la investigación de un incidente de seguridad, deben ser tomados usando procedimientos apropiados de informática forense y cumpliendo los procedimientos de cadena de custodia de dicha información.

b. Las personas encargadas de la gestión de incidentes son responsables de asegurar que todos los documentos recolectados como evidencia en la investigación de un incidente de seguridad, son resguardados y que el proceso de recolección de la evidencia es documentado en la cadena de la custodia.

## 8.11. POLÍTICA ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La Terminal de Transporte S.A. implementa un proceso de continuidad de negocio con la finalidad de mitigar el impacto de acciones como desastres naturales, accidentes, fallas de los equipos y acciones deliberadas de terceros en los cuales la Entidad no tiene injerencia directa, pero establece acciones para poder recuperarse rápidamente y que la operación de la Entidad no se vea comprometida.

Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de

COPIA CONTROLADA

asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada Prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

## 8.12. CUMPLIMIENTO NORMATIVO

### 8.12.1. Cumplimiento de los requisitos legales y contractuales:

#### 8.12.1.1. Derechos de propiedad intelectual (DPI)

a. Todo el software utilizado en las estaciones de trabajo y/o servidores de La Terminal de Transporte S.A. debe estar debidamente licenciado.

b. Los empleados de La Terminal de Transporte S.A. deben cumplir las leyes y las restricciones de derechos de autor definidos por el fabricante de los aplicativos utilizados.

c. La instalación de software en las estaciones de trabajo y/o servidores de La Terminal de Transporte S.A. debe ser aprobado por la Dirección de Recursos Tecnológicos

d. El software desarrollado por o para La Terminal de Transporte S.A. es de propiedad de la organización. El software desarrollado por empleados de la entidad durante su permanencia en la entidad se considera propiedad de La Terminal de Transporte S.A.

e. La Dirección de Recursos Tecnológicos debe realizar revisiones periódicas al software instalado en los equipos de cómputo y servidores de la organización con el fin de identificar software que no cumpla con los derechos de autor y acuerdos de licenciamiento.

f. Todo software que viole los acuerdos de licenciamiento será desinstalado inmediatamente. Los responsables de la instalación, descarga y/o uso de software que viole los acuerdos de licenciamiento serán sujetos de las acciones disciplinarias definidas por parte de la gerencia.

g. Está totalmente prohibido realizar copias parciales o totales de libros y/o software que esté protegido por leyes de derechos de autor.

#### 8.12.1.2. Protección de datos y privacidad de la información personal:

a. La organización debe diseñar e implementar los controles necesarios para proteger los datos personales de empleados o terceros contra acceso y divulgación no autorizada.

#### 8.12.1.3. Prevención del uso inadecuado de los recursos de procesamiento de información:

a. Los recursos de TI utilizados para el procesamiento de información de la organización son para uso exclusivo del negocio. El uso no adecuado de cualquier recurso de TI de la organización o para otros propósitos diferentes a los definidos por el negocio está prohibido. Cualquier actividad no autorizada debe ser reportada a la gerencia.

COPIA CONTROLADA

b. La organización se reserva el derecho de monitorear sin previo aviso el uso de los recursos de TI asignados a los empleados

**8.12.1.4. Revisiones de la seguridad de la información:**

a. 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, debe iniciar el procedimiento de gestión de incidentes de seguridad.

b. 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.

c. 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.

d. 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.

COPIA CONTROLADA