POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Terminal de transportes / Villavicencio

¡Nos vemos pronto!

Modificado:	Revisado:	Aprobado:
JHON FREDY RODRIGUEZ TORRES Ingeniero de Sistemas	**CLAUDIA MILENA RODRÍGUEZ GONZÁLEZ** Coordinadora de Planeación y Gestión de Calidad	**ALCIDES ANDRÉS SOCARRÁS JÁCOME** Gerente
Fecha: 03/08/2021	Fecha: 04/08/2021	Fecha: 05/08/2021

TABLA DE CONTENIDO

PÁG

OBJETIVO

Definir las directrices para garantizar la protección de los activos de información de la Sociedad Terminal de Transportes de Villavicencio S.A, a través de los principios de confidencialidad, integridad y disponibilidad, en cumplimiento de los requisitos legales y reglamentarios.

ALCANCE

La Política de Seguridad de la Información es aplicable a todos los activos de información de la Sociedad Terminal de Transportes de Villavicencio S.A., incluyendo su creación, distribución, almacenamiento y destrucción. Todos los trabajadores, colaboradores, contratistas y terceros que desempeñen alguna labor en la empresa deberán cumplir con las políticas de seguridad y privacidad de la información.

GLOSARIO

ACTIVOS DE INFORMACIÓN: Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades.

CONFIDENCIALIDAD: prevenir la divulgación no autorizada de la información de la empresa.

DISPONIBILIDAD: supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. La información deberá permanecer accesible a usuarios autorizados.

INTEGRIDAD: supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización

SOFTWARE: El software refiere al conjunto de programas, instrucciones y reglas informáticas que gobiernan los procesos que pueden llevar a cabo las computadoras.

HARDWARE: El hardware de la computadora, en términos simples, son los componentes físicos que un sistema de la computadora necesita para funcionar.

IP: Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

BASES DE DATOS: Una base de datos es una colección organizada de información estructurada, o datos, típicamente almacenados electrónicamente en un sistema de computadora. Una base de datos es usualmente controlada por un sistema de gestión de base de datos.

HUB: El Hub es un dispositivo simple con una única misión, la de interconectar los ordenadores de una red local. Estamos por lo tanto ante un punto central de conexión de una red, y suele utilizarse para crear redes locales en las que los ordenadores no se conectan a otro sitio que al resto de ordenadores de la red.

USUARIO: es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema, además se utiliza para clasificar a diferentes privilegios, permisos a los que tiene acceso un usuario o grupo de usuario, para interactuar o ejecutar con el ordenador o con los programas instalados en este.

MARCO NORMATIVO

- Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

- Ley 1273 de 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."

- Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales."

CAPITULO I

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que realiza la Alta Dirección de la Sociedad Terminal de Transportes de Villavicencio S.A. con respecto a la protección de los activos de información, a través de la gestión adecuada y efectiva de la seguridad de la información, garantizando su confidencialidad, integridad y disponibilidad.

La protección de los activos informáticos e información de la Sociedad Terminal de Transportes de Villavicencio S.A. es importante para evitar la fuga de información, ataques informáticos y robo de información, así como poseer soportes de respaldo en la información para así dar confianza a los usuarios.

1.1 DEBERES Y RESPONSABILIDADES DE LOS USUARIOS

- Usar la información de la Sociedad Terminal de Transportes de Villavicencio S.A. únicamente para los propósitos de la organización y en cumplimiento de su labor
- Es obligación de todos los usuarios, reportar al Ingeniero de Sistemas todas las irregularidades que observe o conozca de los sistemas e informática o personas y que puedan afectar la seguridad e integridad de la información.
- No abrir documentos adjuntos o hacer clic en mensajes electrónicos no solicitados.
- No descargar software ilegal (música-material pornográfico). Está estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos, así como copiar software licenciado de la empresa para utilizar en computadores personales.
- No usar el correo electrónico institucional para fines personales.
- No realizar transmisión a terceros de la información de la empresa.
- Es un deber y responsabilidad de cada usuario de la Terminal de Transportes de Villavicencio S.A., hacerse responsable del manejo de sus claves, debe cambiarlas a menudo, no compartirlas, es decir que se hace responsable de la correcta administración de su password, ya que esta es la única forma de identificar a un único usuario. La clave es personal e intransferible.
- El usuario cuando entregue su cargo al momento de retirarse de la empresa deberá dejarla consignada en el acta de entrega a través del formato FR-ADM-35, o cambiar su clave de acceso personal al equipo y programas por cuatro (4) ceros (0000).

- No se debe impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático y a los datos allí almacenados.
- No debe realizar la transferencia no consentida de cualquier activo informático en perjuicio de un tercero.
- No debe divulgar información de carácter confidencial.
- Deberá realizar el acta de entrega y recibo del cargo correspondiente, donde se indique el Software, hardware, periféricos, portátiles, extraíbles, activos informáticos, claves y otros con su correspondiente serial o identificación, a través del formato FR-ADM-35
- No deberá realizar ningún tipo de modificación a su dirección IP y/o configuración de su equipo o del sistema por seguridad de la empresa.
- Es responsabilidad de cada usuario realizar copias de seguridad de la información que maneja periódicamente de acuerdo a la relevancia e importancia.
- Es responsabilidad de cada usuario el adecuado manejo y las consecuencias derivadas del uso de medios de almacenamiento externos a los equipos de cómputo autorizados.
- Toda información que maneje cualquier trabajador, contratista o colaborador que desarrolle un trabajo para la Terminal deberá velar por su buen uso, custodia y confidencialidad, bien sea: Medio magnético, escrito, verbal, visual y otros que perjudiquen el desarrollo de actividad de la empresa.
- Los usuarios están en la obligación en las noches y en los fines de semana, dejar apagados los equipos, las impresoras, periféricos y la UPS.
- El acceso a la sala de sistemas será restringido a personal no autorizado.
- Los usuarios deben conocer y cumplir lo incluido en la Ley 1273 de 2009
- El usuario tiene derecho a recibir capacitación en las políticas de seguridad existentes para su conocimiento y cumplimiento.
- La Terminal de Transportes de Villavicencio S.A., declara la protección de los datos personales recolectados a través de las cámaras de video vigilancia, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, garantizando los principios de confidencialidad, acceso y circulación restringida.
- Para el manejo de las grabaciones del circuito cerrado de monitoreo no se permite sin previa autorización de la Gerencia y Jefatura Operativa, la descarga de videos.

- No se permite la grabación directa desde un celular, cámara de video u otro dispositivo de ningún tipo ni para ningún caso, en la sala del circuito cerrado de monitoreo.
- Es obligación de cada usuario verificar que la información ingresada al sistema sea verificable y confiable.

CAPITULO II

2. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

Artículo 269A: **Acceso abusivo a un sistema informático**: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Artículo 269B: **Obstaculización ilegítima de sistema informático o red de telecomunicación**. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
Artículo 269C: **Interceptación de datos informáticos**. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Artículo 269D: **Daño Informático**. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Artículo 269E: **Uso de software malicioso**. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos

dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO III

3. De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro

medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: **Transferencia no consentida de activos**. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

CAPITULO IV

4. ACTIVOS DE LA EMPRESA

Los activos asociados a los sistemas de información de una organización se pueden clasificar de acuerdo a lo siguiente:

Recursos de información: que en nuestro caso son las bases de datos, manuales de usuario, de procedimiento, planes de continuidad, información archivada y disposiciones de emergencia para la recuperación de la información.

Software: aplicaciones (Condalco, Helissa, Zanin y ORFEO), sistemas operativos (Windows, Oracle y SQL Server) herramientas de desarrollo y utilitarios.

Equipos: servidores, computadores, routers, switches, hubs, PBX, Ups, aires acondicionados y equipos tecnológicos y de comunicaciones.

Servicios: servicios de comunicaciones, de proceso informático, energía eléctrica (iluminación).

4.1 CONTROL DE ACTIVOS E INFORMACIÓN

La Sociedad Terminal de Transportes de Villavicencio S.A. debe tener:

- El inventario de sus activos hardware, software e información.

- No se debe cambiar los equipos de los lugares asignados ya que esto modifica el inventario de activos.
- Todos los equipos deberán estar etiquetados de acuerdo al nivel de jerarquía e información que maneja.
- Los activos informáticos se les realizará su respectivo control, asignando etiquetas.
- Todo producto generado en la Terminal de Transportes de Villavicencio S.A. a través de cualquier activo informático de la Terminal es propiedad de la organización.
- Cada usuario debe utilizar únicamente los activos informáticos asignados para su labor.
- Definición y restricción de páginas web y aplicativas no autorizadas por su contenido o interferencia en el desempeño de las labores asignadas al personal.

CAPITULO V

5. SEGURIDAD FÍSICA Y DE ENTORNO

- La ingesta de bebidas o alimentos sobre los equipos de cómputo es responsabilidad del usuario.
- Cualquier software que se instale en el equipo deberá contar con la respectiva autorización de la Oficina de Sistemas.
- Ningún tipo de equipo informático podrá ser instalado con la configuración por defecto del fabricante o proveedor, ya que esto abre huecos de seguridad, haciendo más vulnerables los sistemas.

5.1 USO DE INTERNET

- El uso de internet puede ser utilizado solamente con fines autorizados y legales.
- El uso de internet y la utilización de activos para su conectividad y explotación, están restringido, y será permitido únicamente para el cumplimiento de la misión institucional y para el desarrollo de las labores de los funcionarios, que por la naturaleza de sus cargos y funciones que requieran de manera justificada por el jefe inmediato.
- La utilización de este recurso se hará dentro del marco que genera la aplicación de principios y valores morales y éticos por parte de todos sus usuarios.

5.2 CONFIDENCIALIDAD

Todos los trabajadores, contratistas, proveedores y terceros, que deban realizar labores para la Sociedad Terminal de Transportes de Villavicencio S.A., sea por medio físico o tecnológico en el que se involucre el manejo de información de la Sociedad, deberán mantener la confidencialidad de la información y no usarse para fines no autorizados.

Igualmente está política de seguridad de la información deberá ser socializada, divulgada y estar disponible en todos los niveles de la organización, con el fin de asegurar su conocimiento y cumplimiento por parte de todos los usuarios de información.

CAPITULO VI

6. REGISTRO DE MODIFICACIONES

FECHA	CAMBIO	NUEVA VERSION
27/10/2014	Se actualizo se modificó se adicionó deberes y responsabilidades de los usuarios, seguridad física y de entorno, administración de sistemas informáticos y uso de internet.	4
30/10/2015	Se actualizo firmas, y se actualizo normatividad	5
15/07/2016	Se adiciono en control de activos e información no se debe cambiar los equipos de los lugares asignados ya que esto modifica el inventario de activos. Se cambió el logo de la empresa y se actualizo firmas.	6
05/08/2021	Se adiciona objetivo, alcance, glosario y marco normativo. Se incluye la palabra activos de información de la empresa, se actualizó y adicionó deberes y responsabilidades de los usuarios, seguridad física y de entorno, administración de sistemas informáticos, uso de internet y confidencialidad.	7