MANUAL DE POLITICAS Y ESTANDARES
DE SEGURIDAD INFORMATICA

TERMINAL DE TRANSPORTES DE CHIQUINQUIRA

NIT. 891.800.571-1

Chiquinquirá

OBJETIVO

Mantener de forma íntegra y disponible la información almacenada en recursos informáticos de LA TERMINAL DE TRANSPORTES DE CHIQUINQUIRA S.A., garantizando autenticidad y confidencialidad en los datos almacenados, asegurando su correcto uso en los recursos de red provistos por la empresa, permitiendo dar disponibilidad y continuidad a la información recolectada por la entidad, cumpliendo la normatividad vigente.

ALCANCE

- Todo el personal vinculado a **LA TERMINAL DE TRANSPORTES DE CHIQUINQUIRA S.A**., en su roll de funcionario o contratista, debe cumplir con los lineamientos establecidos en la PÓLITICA DE SEGURIDAD INFORMATICA, cumpliendo con los procedimientos contenidos en la misma.

- La información contenida, elaborada en recursos tecnológicos de LA TERMINAL DE TRANSPORTES DE CHIQUINQUIRA S.A., se entenderá como activo informático propiedad de la Empresa.

POLITICAS ESPECÍFICAS

Con el fin de reglamentar medidas de control para el uso correcto y adecuado tanto de sistemas de información, como de los recursos de red y otros componentes tecnológicos, a continuación se mencionan políticas de cumplimiento obligatorio.

Confidencialidad

- Los funcionarios o contratistas de LA TERMINAL DE TRANSPORTES S.A., deben tener confidencialidad con toda la información conocida, generada o almacenada en el desempeño de sus funciones, principalmente la relacionada con: empleados, proveedores, accionistas, contratistas, clientes, y cualquier información considerada como confidencial para la Entidad.

Control de Acceso

1. Está prohibida la divulgación de contraseñas adquiridas en la Empresa, es responsabilidad de los usuarios conocer y salvaguardar dicha información, garantizando plena identificación y autoría en la creación y modificación de documentos, registros, trabajos y demás tareas asignadas.

2. En caso de ausencia, los empleados deben garantizar el bloqueo del equipo de cómputo, con el fin de evitar suplantación de identidad, obligando a la digitación de una contraseña, previo uso del ordenador.

3. Las cuentas de acceso tendrán vigencia de acuerdo con el vínculo contractual del personal con la empresa.

4. A todos los funcionarios o contratistas que tengan acceso a los sistemas de información o de red de la empresa, se les asignará usuario y contraseña personal e intransferible.

5. Se debe notificar a los responsables de administrar sistemas o recursos de red, desvinculaciones o cambio de responsabilidades, para deshabilitar o modificar las cuentas de usuario contenidas en el entorno de red.

6. El acceso a sistemas de información o servicios de red, deberá ser aprobado por la Gerencia, relacionando perfil, restricciones y vigencia.

7. Se establecen controles de bloqueo al sistema de modo automático, al alcanzar un periodo de inactividad considerable.

8. El uso de claves de bases de datos debe ser administrado en custodia compartida por personal de la misma área, garantizando disponibilidad de acceso y de forma independiente a la disponibilidad del personal responsable del tratamiento de los datos.

Tratamiento de datos personales

- La transferencia o almacenamiento de información que se encuentren contenidos en hojas de cálculo o documentos electrónicos, deben realizarse tomando precauciones de confidencialidad en favor de la seguridad de la

información, como proteger el acceso al archivo con una clave compartida o en información más clasificada con encriptación.

- Es deber de los funcionarios reportar al oficial de protección de datos personales, cualquier novedad, disponibilidad, vulnerabilidad y otros cambios en datos personales contenidos en bases de datos de la empresa.

- Al transferir información personal, se deben tomar medidas preventivas necesarias para evitar perdida de confidencialidad, integridad y disponibilidad de la información.

- Se deben cumplir las políticas de tratamiento de datos personales particulares a cada una de las bases de datos, y respetar la finalidad con que los datos fueron recaudados.

- Los funcionarios deben abstenerse de exceder las funciones y responsabilidades sobre datos personales al extraer, copiar, compartir, duplicar, transferir y/o almacenar información de datos personales de los sistemas de información de la empresa sin previa autorización del responsable de la base de datos.

Uso de correo electrónico

- Todo funcionario que requiera uso de buzón de correo electrónico, podrá recibir documentos, cartas y demás a nombre de la Empresa, usando una cuenta de correo empresarial con el dominio terminalchiquinquira.com.

- El identificador de la cuenta de correo electrónico debe ser impersonal y corporativo, en casos específicos será personalizado a solicitud formal y justificada por un rol directivo.

- Se puede monitorear y acceder al contenido de los buzones de correo institucional, cuando la Empresa lo determine conveniente, teniendo en cuenta que la información contenida en las cuentas de correo es propiedad de la Entidad.

- Toda comunicación usando este medio, deberá llevarse dentro de las premisas de respeto y buenas costumbres, aportando a la buena imagen de la Empresa.

- Los usuarios de buzones no deben compartir o transferir información de archivos, fuera del dominio terminalchiquinquira.com, sin controles de acceso.
- Se inactivara la cuenta de usuario y se cambiará la contraseña, a todo funcionario que se retire de la empresa, para restringir el acceso del ex funcionario.

- Los usuarios del correo empresarial deben asegurar el correcto uso de la información contenida en las cuentas asignadas, haciendo buen uso de la capacidad de almacenamiento del mismo.

- EL correo electrónico solo será asignado para asuntos laborables, no podrá ser usado para fines personales, redes sociales, cadenas entre otros.

- Los funcionarios no podrán utilizar servicios de almacenamiento en nube cuentas de correo personal para compartir información de la empresa.

- La empresa tiene la facultad de restringir las capacidades de la cuenta de correo, teniendo en cuenta el perfil y las responsabilidades del usuario en la misma.

- A quien se le asigne correo electrónico empresarial deberá hacer mantenimiento preventivo del buzón (limpieza de bandejas y control en espacio de almacenamiento).

Servicios de internet

- Está prohibido realizar escaneo o control al sistema, redes o seguridad de la información, a menos que exista una autorización por parte de la directiva, o que sea una función de su actividad de trabajo.

- El servicio de internet no podrá ser utilizado para navegar en sitios que no estén relacionados a las funciones propias del cargo.

- Está prohibido el acceso a páginas con contenido ilícito, pornográfico, racista, sexual, o cualquier otro material que atente contra la dignidad y los principios morales.

- El servicio de internet podrá restringir acceso a sitios que a consideración del administrador del sistema no sean apropiados o sean innecesarios para la actividad laboral.

Servicios de la red inalámbrica

- La red inalámbrica debe estar siempre independiente de la red de Computadores de la entidad, y brindará un servicio restringido, solamente a equipos portátiles y dispositivos de la empresa.

- En equipos autorizados para conectarse a la red inalámbrica, deberá hacerse seguimiento y control con el fin de no poner en riesgo la empresa con software malicioso.

- Se autoriza el servicio de red inalámbrica a equipos que hayan sido autorizados únicamente por La Gerencia.

Uso de Software

- Los funcionarios podrán solicitar al personal de soporte de tecnología la instalación y capacitación de software especializado para protección de datos personales sensibles o confidenciales de la empresa.

- Solo se podrá instalar en los equipos de cómputo de la empresa software licenciado o de uso libre, justificado por La Gerencia, y evaluado por el personal de soporte de tecnología para evitar software malicioso, virus y demás riesgos informáticos.

- La compra de software, sistema de información, equipos de cómputo, equipos de red, estará sujeta al visto bueno del responsable del proceso de tecnología, para garantizar la integración con la arquitectura empresarial.

- Los daños causados en equipos informáticos, así como en los sistemas de información, por malware troyanos y demás software malicioso, que sean generados por la descarga activación o instalación de software no autorizado por la empresa, será causal para acciones disciplinarias o penales, según el caso.

- Está prohibido descargar desde internet, o desde cualquier otra fuente, copiar, almacenar, reproducir o instalar, videos o películas, exceptuando las actividades relacionadas con fines laborales.

- Está prohibido el uso de recursos informáticos para uso, reproducción o copia de material no autorizado por el propietario de los derechos de autor o por su representante.

- Las mejoras al software (instalación, modificación, reparación, desinstalación) en los equipos de cómputo de la empresa, deberán ser registradas como requerimientos del sistema.

- La instalación y descarga de software en los equipos de cómputo de la Empresa, esta exclusivamente permitida al personal de soporte de tecnología.

Uso de Equipo de Cómputo, eléctrico o electrónico

- El funcionario o contratista es responsable del el uso adecuado del equipo de cómputo y/o dispositivo móvil proporcionado por la Empresa; reportando oportunamente al personal de soporte de tecnología las fallas evidenciadas durante la operación del mismo.

- Se asignará un único equipo de cómputo para cada usuario, de no ser esto posible, se buscará optimizar los recursos de cómputo con que se cuente.

- El funcionario o contratista a quien ha sido proporcionado el equipo de cómputo portátil y/o dispositivos móviles debe tomar las precauciones necesarias para prevenir el hurto o pérdida del equipo, el acceso no autorizado por terceros a la información almacenada en el equipo fuera de las instalaciones de la Empresa.

- Los computadores, dispositivos móviles, correos, internet y demás recursos o servicios de la Empresa no se podrán usar con fines delictivos (terrorismo, soborno, chantaje o cualquier uso que viole leyes de carácter local, nacional o internacional).

- El uso inapropiado comprobado que se dé a los equipos ofimáticos de la empresa como por ejemplo derrame de líquidos en portátiles o teclados,

daños por golpes o defectos causados que conduzcan a la pérdida parcial o total del activo será reportado al ente disciplinario correspondiente.

- **Se deberá apagar adecuadamente el equipo de cómputo y periféricos, una vez que concluya el horario laboral.**

- Todo usuario es responsable de conocer el manejo del equipo de cómputo asignado, los sistemas de información y servicios de red que utilizará y de solicitar a quien corresponda la capacitación o entrenamiento en el uso de los mismos.

- Las tomas de energía regulada (de color naranja) están restringidas únicamente para la conexión de equipo de cómputo (computadores, monitores).

Acceso restringido

- ✓ La Gerencia podrá solicitar y justificar formalmente solicitudes para excepciones a accesos restringidos, las cuales serán evaluadas y autorizadas por el responsable del proceso o del activo correspondiente.

- ✓ Está prohibido suministrar información perteneciente a la configuración de sistemas de información, servicios de comunicación y equipos, a terceros fuera de la empresa.

- ✓ La Empresa establecerá áreas físicas y servicios de acceso restringido identificados y delimitados por barreras físicas, lógicas, monitoreados y protegidos con mecanismos de control de acceso que serán registrados y auditados sin previa autorización del usuario o visitante.

- ✓ Se controlará por el personal de soporte de tecnología la utilización de dispositivos de almacenamiento externo (USB, DVD, CD, Discos duros externos).

Copias de Seguridad

- o Las copias de seguridad de archivos ubicados en equipos de cómputo, son responsabilidad en conjunto del usuario y del administrador del sistema, y

deberán coordinar fecha, almacenamiento y la obtención (cuando aplique) de las copias de respaldo de los mismos.

- El personal de soporte de tecnología será responsable del respaldo y continuidad de la información en las carpetas ubicadas y organizadas de acuerdo a las políticas establecidas para control de back up en el equipo de cómputo.

- Se deben acatar las indicaciones y recomendaciones brindadas por el personal de soporte de tecnología de la Empresa sobre la ubicación, organización de carpetas y de toda información o documento creado o recibido, mediante medios electrónicos, servicios de red o mediante los aplicativos o sistemas de información usados en la Empresa.

Manejo de Incidentes y Controles de Cambio

- El reemplazo de cualquier componente en sistema de información o recurso de red de la empresa con alta probabilidad de generar incidentes que produzcan pérdida de confidencialidad, disponibilidad e integridad de los datos debe ser gestionado por un plan de cambio.

- Los funcionarios o responsables de equipos informáticos deberán reportar de manera formal los incidentes que afecten la capacidad de procesamiento de datos y que puedan incidir en perdida de información o afectación en las funciones del cargo.

- Los incidentes sobre sistemas de información o servicios de red que causen perdida de confidencialidad, integridad o disponibilidad, podrán ser puestos en conocimiento de organismos de control o vigilancia, sujeto a la aprobación del representante legal.

- Los responsables de procesos o de activos de información deberán notificar oportuna y formalmente, o mediante un caso en la mesa de ayuda a la Dirección de TIC, cualquier riesgo o novedad relacionada con la pérdida de confidencialidad, integridad o disponibilidad de información de las bases de datos de la empresa.

Adquisiciones

- Toda iniciativa de reemplazo de sistemas de información dentro de la empresa debe ser valorado y justificada, determinado el presupuesto estimado y los indicadores que se esperan mejorar como producto del cambio del sistema información.

- La adquisición o reposición de un componente de comunicaciones (switches, routers, firewall, WAP) deberá ser aprobada y controlada por el personal de tecnología e informática.

- Las implementaciones de software como sistema de información que implican un esfuerzo puntual con recursos y tiempos limitados deben abordarse con una metodología de control de proyecto que permita garantizar el cumplimiento de las restricciones de tiempo, costo y el logro de los entregables.

- Toda solicitud de repuestos, dispositivos externos y/o reemplazos relacionados con ofimática, comunicaciones, deben de ser requeridos por la herramienta de gestión de tecnología, para que sea aprobada dicha compra.

Continuidad del Negocio

- Teniendo en cuenta el análisis de impacto en el negocio, a partir de la pérdida en servicios de red o en sistemas de información, se dispondrán de recursos físicos y tecnológicos para la activación de planes de contingencia y recuperación ante desastres, con el fin de dar continuidad a los procesos claves del negocio.

- El personal deberá capacitarse y seguir las instrucciones y acciones correspondientes en la activación de planes de contingencia y recuperación ante desastres.

Sanciones Disciplinarias

- El funcionario que haga uso inapropiado de equipos de cómputo, sistemas de información, servicios de red, accesos restringidos de la Empresa, incumpla o sobrepase la política de seguridad de la información, incurrirá en

sanciones disciplinarias, las cuales se aplicaran teniendo en cuenta la gravedad de la falta, así como de su reincidencia. Tomando como base lo establecido en el reglamento interno o en documentos que soporten los acuerdos de la relación contractual.

- En caso de configurarse las tipologías enumeradas en la Ley 1273 de 2009, se procederá a denunciar ante las autoridades competentes a el(los) funcionarios o contratista(s), vinculados en la falta.