**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**

**ALCANCE DE LAS POLÍTICAS**

Las políticas definidas el presente documento aplican a todos los funcionarios de Transportes Camiones y Camiones LTDA.

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

TC&C: Transportes Camiones y Camiones LTDA.

Política: son instrucciones mandatorias que indican la intención de la gerencia respecto a la operación de la empresa

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones).

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Usuarios: Todas aquellas personas naturales o jurídicas, que no son funcionarios de TC&C, y que por las actividades que realizan, deban tener acceso a Recursos Informáticos

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

**DESCRIPCIÓN DE LAS POLITICAS**

**POLITICA 1: ACCESO A LA INFORMACIÓN**

Todos los funcionarios de TC&C deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.

El uso de los sistemas de información de la empresa debe terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la empresa.

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

**POLITICA 2: ADMINISTRACION DE CAMBIOS**

Todo cambio que afecte los recursos informáticos, debe ser requerido por los usuarios y aprobado formalmente por el (la) analista de administración y control interno con VoBo de la gerencia general.

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

**POLITICA 3: SEGURIDAD DE LA INFORMACION**

Los funcionarios de TC&C son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la empresa, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios de TC&C no deben suministrar información de la empresa a ningún ente externo sin la autorización de su jefe inmediato.

Los funcionarios de TC&C deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva del trabajo realizado. Una vez retirado el funcionario, debe comprometerse a no utilizar, la información generada o conocida durante la gestión en la empresa.

**POLITICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMATICOS**

El sistema de correo electrónico, grupos de charla y utilidades asociadas de la empresa debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario.

La empresa se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, el funcionario o autorizará a la empresa para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

Los funcionarios de la empresa deben utilizar el servicio de Internet única y exclusivamente para las actividades relacionadas con su cargo.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente reportarlo a él (la) analista de administración y control interno, no utilizar el computador y desconectarlo de la red.

**POLITICA 5: SEGURIDAD EN RECURSOS INFORMATICOS**

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios de TC&C son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Cada usuario debe actualizar sus contraseñas cada 2 meses y reportarlas al analista de administración y control interno.

**POLITICA 6: SEGURIDAD EN COMUNICACIONES**

Los computadores de TC&C se conectarán de manera directa con computadores de entidades externas, previa autorización de él (la) analista de administración y control.

**POLITICA 7: SEGURIDAD PARA USUARIOS TERCEROS**

Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, estos eventos deben ser aprobados por él (la) analista de administración y control interno y por la gerencia general.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y por él (la) analista de administración y control interno y por la gerencia general.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la empresa.

La empresa se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La empresa se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la entidad.

**POLITICA 8: SOFTWARE UTILIZADO**

Todo software que utilice TC&C será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Debe existir una cultura informática al interior de la empresa que garantice el conocimiento por parte de los funcionarios las implicaciones que tiene el instalar software ilegal en los computadores de TC&C.

**POLITICA 9: ACTUALIZACION DE HARDWARE**

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización de él (la) analista de administración y control y la gerencia general.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa de él (la) analista de administración y control.

**POLITICA 10: ALMACENAMIENTO Y RESPALDO**

Toda la información de TC&C deberá ser almacenada y respaldada con una copia interna y una copia externa para garantizar su disponibilidad. La copia externa será salvaguardad por la gerencia general.

Semanalmente se correrá el proceso de actualización de copias de respaldo. Ver insctructivo.

**POLITICA 11: CONTINGENCIA**

La gerencia general de la empresa debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

**POLITICA 12: SEGURIDAD FISICA**

La Entidad deberá contar con los mecanismos de control de acceso tales como puertas de seguridad.

Los visitantes de las oficinas de la entidad deben ser escoltados durante todo el tiempo por un empleado autorizado.

Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la oficina de informática.

Los equipos de microcomputadores ( PCs, servidores ,equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

**POLITICA 13: ESCRITORIOS LIMPIOS**

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, usb memory key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.