1. INTRODUCCIÓN

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de la Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.
En nuestro país no existe una sola institución que no se haya visto sujeta a los ataques en sus instalaciones, tanto desde el interior como del exterior.

2. OBJETIVO

Establecer los estándares, protocolos, métodos, reglas y herramientas apropiadas para garantizar el adecuado funcionamiento de la gestión informática, así mismo, minimizar los posibles riesgos a los que pueda estar sometida la infraestructura tecnológica de la organización.

3. ALCANCE

La presente política aplica para el proceso de gestión informática de las cinco compañías del Grupo Mototransportar (Mototransportar, Mototransportamos, Motoseguridad, Refrilogística y Tramitar Documentos)

4. POLÍTICA DE SEGURIDAD INFORMÁTICA

El Departamento de Sistemas e Informática del Grupo Mototransportar (Mototransportar, actualmente está conformado por 2 funcionarios y la Empresa Carga Control S.A.S., los cuales compelen distintas funciones referentes al soporte y mantenimiento de la plataforma tecnológica y desarrollo de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de la red; dado a esta razón ha sido necesario emitir políticas particulares para el conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por la Organización. Así pues, este apartado contiene una clasificación de estas políticas, y son:

5. EQUIPOS

5.1 Instalación de Equipo de Cómputo.

Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores, Impresoras, escáner y otros equipos o accesorios), que estén o sean conectados a la red de La Organización, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite el departamento de Sistemas e Informática.
El Departamento de Sistemas e Informática debe tener un registro de todos los equipos propiedad de la Organización. (Hojas de Vida).
El equipo de la Organización que sea de propósito específico y tenga una misión crítica asignada (Servidores, Switch, Rack), requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica y la normatividad legal aplicable.
Los funcionarios del Departamento de Sistemas e Informática deben dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, así como elaborar actas de entrega de equipos de cómputo y llevar su respectivo control.
La protección física de los equipos corresponde a quienes en un principio se les asigna (Acta de Entrega), y es su deber notificar los movimientos (en caso de que existan), a los funcionarios del Departamento de Sistemas e Informática.

5.2 MANTENIMIENTO DE EQUIPOS DE CÓMPUTO.

Al Departamento de Sistemas e Informática, le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.
En el caso de los equipos atendidos por terceros, El Departamento de Sistemas e Informática debe coordinar y velar por el cuidado y preservación del mismo, para lo cual debe gestionar el registro de mantenimientos, según los respectivos procedimientos.
Actualización de los equipos. Todo el equipo de cómputo (computadoras personales, estaciones de trabajo, servidores y demás relacionados), y los de telecomunicaciones que sean propiedad de la Organización deben procurarse sean actualizados tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

5.3 REUBICACIÓN DEL EQUIPO DE CÓMPUTO

La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el Departamento de Sistemas e Informática emita para ello.

En caso de existir personal técnico de apoyo, éste debe notificar los cambios tanto físicos como de software que realice. Dando aviso al Departamento de Sistemas e Informática, quien finalmente registra los mencionados cambios en el inventario.
El equipo de cómputo a reubicar sea propiedad de la compañía o externo, se debe hacer únicamente bajo la autorización del responsable, contando con la disponibilidad del lugar a donde se hará la ubicación con los medios necesarios para la instalación final del equipo.

6. DEL CONTROL DE ACCESOS

6.1 Del Control de Acceso a la Organización

El Departamento de Sistemas e Informática, debe proveer el Hardware – Software para el control de Ingreso, y capacitar el personal encargado del registro de cada usuario, configuración de horarios, toma de huellas y registro fotográfico.

6.2 Del Control de Acceso a Los Aplicativos Administrativos de la Organización.

El Departamento de Sistemas e Informática debe proporcionar a cada persona que lo requiera, un Usuario y una clave únicos para el ingreso a las aplicaciones de la Organización.
Corresponde al Departamento de Sistemas e Informática asignar a cada usuario registrado en el sistema de la organización los permisos necesarios para su correcto desempeño.
Para reemplazos de vacaciones, cambios de funcionarios, corresponde al Departamento de Talento Humano en coordinación con el Área de Sistemas e Informática asignar permisos extras a los usuarios a quien asigne la Dirección General para ocupar estos cargos.

6.3 Del Acceso a Áreas Críticas.

El Departamento de Sistemas e Informática debe proveer la infraestructura de seguridad requerida con base en las necesidades específicas de cada área.

6.4 Del control de acceso al equipo de cómputo.

Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Dirección del Departamento de Sistemas e Informática tiene la facultad de acceder a cualquier equipo de cómputo que no esté bajo su supervisión.
Cada equipo de cómputo conectado a la Red del Grupo Mototransportar y Filiales, tiene asignado un usuario y contraseña único dentro del Sistema de la Organización.
Cada Usuario configurado en cada equipo de la Organización tiene configurado un vencimiento

6.5 Del control y asignación de cuentas individuales

Para efectos de garantizar el control de las cuentas individuales, a cada empleado se le asigna un usuario y una clave de acceso a las aplicaciones administrativas, que según la criticidad del cargo o del proceso se cambian y se monitorean cada 30 días. Por seguridad, estas claves deben ser numéricas o alfanuméricas.
Para ciertos cargos que no sean de mayor criticidad el cambio puede ser superior a 30 días. Es responsabilidad del Jefe de Sistemas ejercer de manera directa los controles que se requieran sobre este particular.

6.6 Del control de acceso y salida de información.

A manera de control y prevención sobre el abuso o uso inadecuado respecto del acceso o salida de información mediante correos electrónicos, utilización de USB, discos extraíbles y demás dispositivos en medios magnéticos, la Organización tiene contemplado un otro sí, donde todos los empleados manifiestan el compromiso de abstenerse de hacer uso indebido de la información de propiedad de la empresa.
En el mismo otro sí, el cual hace parte integrante del contrato de trabajo, además de las sanciones de tipo disciplinario contenidas en el reglamento interno de trabajo, igualmente se contemplan las sanciones de tipo penal, de conformidad con lo dispuesto en la ley 1273 de 2009 para hacer respetar y salvaguardar la integridad de la información de propiedad de la organización.

6.7 Del control de acceso local a la red.

El Departamento de Sistemas e Informática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
El Departamento de Sistemas e Informática es el responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.
Dado el carácter unipersonal del acceso a la Red de Mototransportar y Filiales, El Departamento de Sistemas e Informática debe verificar el uso responsable, de acuerdo al Reglamento para la utilización de la red.
El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos) conectado a la red es administrado por El Departamento de Sistemas e Informática.
Todo el equipo de cómputo que esté o sea conectado a la Red de Mototransportar y Filiales, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe sujetarse a los procedimientos de acceso que emite El Departamento de Sistemas e Informática.

6.8 De control de acceso remoto.

El Departamento de Sistemas e Informática es el responsable de proporcionar el servicio de acceso remoto (Usuario y Contraseña) y las normas de acceso a los recursos informáticos disponibles.

Para el caso especial de los recursos de SERVIDORES a terceros deben ser autorizados por la DIRECCIÓN GENERAL.
El usuario de estos servicios debe sujetarse al Reglamento de uso de la Red de Mototransportar y Filiales y en concordancia con los lineamientos generales de uso de Internet.
El acceso remoto que realicen personas ajenas a la institución debe cumplir las normas que emita El Departamento de Sistemas e Informática.

6.9 De acceso a los sistemas administrativos.

Tendrá acceso a los sistemas administrativos sólo el personal de Mototransportar y Filiales o persona que tenga la autorización por la DIRECCIÓN GENERAL DE LA ENTIDAD.
El control de acceso a cada sistema de información de la Dirección Administrativa debe ser determinado por la unidad responsable de generar y procesar los datos involucrados.

6.10 Del Acceso a Internet.

Sólo se permiten servidores de páginas autorizados por, EL Departamento de Sistemas e Informática.
Los accesos a las páginas Web a través de los navegadores, deben sujetarse a las normas (Proxy), que previamente se manifiestan en el Reglamento de acceso a la red de Mototransportar y Filiales (Pendiente por Documentar).
A los responsables de los servidores Web, corresponde la verificación de respaldo y protección adecuada.
El material que aparezca en la página de Internet de Mototransportar y Filiales debe ser probado por la oficina de Comunicaciones y Publicidad, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
En concordancia con la libertad de investigación, se acepta que en la red (Intranet) de Mototransportar y Filiales conectada a Internet, pueda publicarse información individual sin autorización (siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales paraestatales).
El Departamento de Sistemas e Informática tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

7. DE UTILIZACIÓN DE LOS RECURSOS DE LA RED

Los recursos disponibles a través de la Red de Mototransportar y Filiales son de uso exclusivo para asuntos relacionados con las actividades de la entidad.
El Departamento de Sistemas e Informática es el responsable de emitir y hacer seguimiento al Reglamento para el uso de la Red (Pendiente por Documentar).
El Departamento de Sistemas e Informática debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas y ecológicas de la institución.

8. DEL SOFTWARE

8.1 De la adquisición del Software

La Adquisición de Software se hace en concordancia con la Dirección General y El Departamento de Sistemas e Informática, quienes son los departamentos oficiales de la organización para establecer los mecanismos de procuración de sistemas informáticos.
Del presupuesto de los proyectos que se autoriza la dirección general, se otorga un rubro que debe ser aplicado para la adquisición de sistemas de información licenciados, o bien sea mediante el desarrollo de sistemas de información a la medida.
De acuerdo con el MINISTERIO DE LAS TI, la Dirección General en conjunto con El Departamento de Sistemas e Informática, propicia la adquisición de licencias en cantidad, para obtener economías de escala en concordancia con el plan de austeridad promulgado mediante las políticas económicas gubernamentales.
Corresponde al Departamento de Sistemas e Informática emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.
De acuerdo a los objetivos globales del Departamento de Sistemas e Informática, esta dependencia debe propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.
En cuanto a la paquetería sin costo debe respetarse la propiedad intelectual intrínseca del autor.
El Departamento de Sistemas e Informática debe promover y propiciar que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
El Departamento de Sistemas e Informática debe promover el uso de sistemas programáticos que redunden en la independencia de la institución con los proveedores.

8.2 De la instalación del Software

Corresponde al Departamento de Sistemas e Informática emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.
El Departamento de Sistemas e Informática es el responsable de brindar asesoría y supervisión para la instalación de software informático, asimismo para el software de Monitoreo, Contable, Administrativo, telecomunicaciones, telefonía Ip.
La instalación de software que desde el punto de vista del Departamento de Sistemas e Informática pudiera poner en riesgo los recursos de la institución no está permitida.
Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).
La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al Departamento de Sistemas e Informática.

8.3 De la actualización del Software

Corresponde al Departamento de Sistemas e Informática autorizar cualquier adquisición y actualización del software.
Corresponde al Departamento de Sistemas e Informática, estar pendiente que los equipos de cómputo que cuentan con Software antivirus y S.O. estén actualizándose periódicamente.

8.4 De la auditoría del Software instalado

Corresponde al Departamento de Sistemas e Informática auditar periódicamente que el software instalado en los equipos cumpla con los parámetros establecidos, y que no haya sido modificado por los usuarios.

8.5 Del Software propiedad de la Organización

Todo Software adquirido por la institución sea por compra, donación o cesión es propiedad de la institución y por tanto debe mantener los derechos que la ley de propiedad intelectual le confiera.
Todos los sistemas desarrollados (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de Carga Control S.A.S se deben mantener como propiedad de la institución respetando la propiedad intelectual del mismo.
Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución, el cual debe preservarse.
Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución (Syscar, Seguridad, Trámites) deben estar resguardados.
Corresponde al Departamento de Sistemas e Informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas de Desarrollos propios en conjunto con Carga Control S.A.S.
El Departamento de Sistemas e Informática le corresponde administrar los diferentes tipos de licencias de software, además debe vigilar su vigencia en concordancia con la política informática.

9. DE LA SUPERVISIÓN Y EVALUACIÓN

Para efectos de que la institución disponga de una red con alto grado de confiabilidad, es necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen (Acceso a Páginas Web, Procesos críticos del software administrativo, Software de Monitoreo de Vehículos "Sígueme").
Los sistemas considerados críticos, deben estar bajo monitoreo permanente.

10. GENERALIDADES.

Cada uno de los departamentos debe emitir los planes de contingencia que correspondan a las actividades críticas que realicen.
Debido al carácter confidencial de la información, el personal del Departamento de Sistemas e Informática debe conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

11. SANCIONES.

Cualquier violación a las políticas y normas de seguridad debe ser sancionada de acuerdo a la escala de faltas contenidas en el Reglamento Interno de Trabajo aprobado por la organización, el cual se encuentra publicado y socializado de conformidad con la normatividad legal vigente.
Las sanciones pueden ser desde una llamada de atención, suspensiones o terminación de contrato, dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.
Corresponde al Comité de Informática o a la Dirección de Talento Humano de la compañía, hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.
Todas las acciones en las que se comprometa la seguridad de la Red del Grupo Mototransportar y que no estén previstas en esta política, deben ser revisadas por la Dirección General, para documentar mecanismos que permitan blindar la seguridad de la misma, de conformidad con la legislación legal vigente aplicable.
En cuanto a los daños a la infraestructura tecnológica, interceptación ilegítima de sistema informático o red de telecomunicación, suplantación de sitios Web para capturar datos personales, acceso abusivo a un sistema informático y demás delitos informáticos, la compañía se acoge a lo dispuesto en la ley 1273 de 2009 para hacer respetar y salvaguardar la integridad de su plataforma informática.