## 1. PROPÓSITO

Establecer en AREA LOGISTICA CARGO S.A.S políticas de seguridad que permitan operar de una forma confiable, evaluando y administrando los riesgos que se puedan presentar.

## 2. CAMPO DE APLICACIÓN

Aplica para los criterios de Seguridad institucional, Seguridad física, Manejo y control del centro de cómputo, Control de usuarios y Lineamientos legales.

## 3. CONDICIONES GENERALES

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el área T.I (Tecnologías de la información), nombre asignado al Área de Sistemas.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de Área Logística. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por el área T.I al personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

### 3.1 Evaluación de las Políticas

Las políticas tendrán una revisión periódica semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias; con el objetivo de garantizar la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones en la compañía.

### 3.2 Seguridad Institucional

Toda persona que ingresa como usuario nuevo a Área Logística para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

### 3.3 Asignación y/o cancelación de usuarios.

Todo el personal nuevo de la compañía, deberá ser notificado al área de T.I, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

### 3.4 Capacitación en seguridad informática

Todo funcionario nuevo en Área Logística deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

**Nota:**
Se consideran violaciones graves y objeto de sanciones: el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

### 3.5 Protección de la información y de los bienes informáticos

Para el acceso a los sitios y áreas restringidas se debe notificar al área de T.I para la autorización correspondiente, y así proteger la información y los bienes informáticos.

- El usuario o funcionario deberán reportar de forma inmediata al área de T.I cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
- El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignado.

### 3.6 Controles de acceso físico

- Toda persona que tenga acceso a las instalaciones de Área Logística, deberá registrar al momento de su entrada, el equipo de cómputo, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.
- Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de Área Logística únicamente con la autorización de salida del área de T.I, anexando el

comunicado de autorización del equipo debidamente firmado por el director del área de T.I.

### 3.7 Seguridad en áreas de trabajo

Los Centros de Cómputo de Área Logística son áreas restringidas, por lo que solo el personal autorizado por el área de T.I puede acceder a él.

### 3.8 Protección y ubicación de los equipos

- Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del área de T.I, en caso de requerir este servicio deberá solicitarlo.
- El Área de T.I será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores de Área Logística.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.
- Se debe mantener el equipo informático en un lugar limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal del área de T.I.
- Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación a la Oficina T.I. a través de un plan detallado.
- Cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al área de T.I a través de un plan detallado.
- Queda terminantemente prohibido que el usuario o funcionario distinto al personal del área de T.I abra o destape los equipos de cómputo.

### 3.9 Mantenimiento de equipos

- Únicamente el personal autorizado por el área de T.I podrá llevar a cabo los mantenimientos y reparaciones al equipo informático.
- Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

### 3.10 Pérdida de Equipo

- El funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- El préstamo de laptops o portátiles tendrá que solicitarse al área de T.I, con el visto bueno del director de sistemas o el jefe inmediato.
- El servidor o funcionario deberá dar aviso inmediato al área de T.I, de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

### 3.11 Uso de dispositivos extraíbles

- El área de T.I, velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
- Cada Jefe de Área o dependencia debe reportar al área de T.I el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.
- El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.
- Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el área de T.I con el respectivo visto bueno del director de sistemas o en su defecto de su Jefe inmediato.
- Todo funcionario o servidor de Área Logística deberá reportar al área de T.I el uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

### 3.12 Daño del equipo

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

### 3.13 Administración de Operaciones en los Centros de Cómputo

- Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de Área Logística. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna o redes externas como internet.
- Los usuarios y funcionarios de Área Logística que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.
- El área de T.I en cabeza del director de la misma, establecen las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.
- Cuando un funcionario no autorizado o un visitante requieran ingresar a la Sala donde se encuentren los Servidores, debe solicitar mediante comunicado interno debidamente firmado y autorizado por el Jefe inmediato de su sección o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno del área de T.I, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del área de T.I.
- Todo equipo informático ingresado a los Centros de Cómputo restringidos deberá ser registrado en el libro de visitas.
- Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
- El director del área de T.I deberá solicitar a la gerencia los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

### 3.14 Uso de medios de almacenamiento

- Los usuarios y servidores de Área Logística deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.
- Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones de Área Logística serán registradas y podrán ser objeto de auditoria.

### 3.15 Adquisición de software.

- Los usuarios y funcionarios que requieran la instalación de software que sea o no propiedad de Área Logística, deberán justificar su uso y solicitar su autorización por el área de T.I con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.
- Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, puestos de trabajo, servidores, o cualquier equipo conectado a la red de Área Logística, que no esté autorizado por el área de T.I.
- El área de T.I, tiene a su cargo la tarea de informar periódicamente a la gerencia la piratería de software, utilizando todos los medios de comunicación disponibles: Página WEB, Emails, Carteleras y Boletines. Debemos considerar también la publicación de las posibles sanciones o multas en los que se puede incurrir.
- AREA LOGISTICA CARGO S.A.S, cuenta con un office legal, lo que nos permite garantizar la legalidad de los programas adquiridos. Cualquier otro "software" requerido, y que no pueda ser provisto por la compañía Microsoft, será adquirido a otro proveedor debidamente certificado, el cual deberá entregar al momento de la compra, el programa y la licencia del software con toda la documentación pertinente y necesaria que certifique la originalidad y validez del mismo.
- El control de manejo para las licencias y el inventario de los Medios, paquete de CD´s será responsabilidad del área de T.I.
- El área de T.I tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Institución.
- En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.
- Deben mantener un inventario de equipos físicos y de los programas instalados y pueden borrar o instalar programas o software autorizados y legalmente licenciados. Cualquier otra petición de software deberá ser tramitada a través del área de T.I, utilizando el debido formato.
- El área de T.I ofrecerá capacitaciones al personal administrativo en el manejo y uso de las Tecnologías de Informática y Computación, para de esta manera convertir estos en herramientas efectivas de trabajo, y que apoyen la labor en el Interior de la compañía. La capacitación de nuestro personal estimula en gran medida la utilización de los programas adquiridos legalmente, evitando la práctica indebida de utilizar y la proliferación software no autorizado (pirata).

### 3.16 Licenciamiento de Software

Para el Control de Licenciamiento de Software: Área logística cuenta con un office legal, además como política de seguridad se tiene establecido la prohibición de instalar software y programas no autorizados y sin licencia. El área de T.I realiza

semanalmente un inventario físico de los programas y software instalados en cada uno de los computadores de la compañía.

### 3.17 Identificación de incidentes

- El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de T.I lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de los directos responsables, el usuario o funcionario informático deberá notificar al área de T.I.
- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de Área Logística debe ser reportado al área de T.I.

### 3.18 Administración de la Red

Los usuarios de Área Logística Cargo no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización del área de T.I.

### 3.19 Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el área de T.I, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red de Área Logística, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

### 3.20 Uso del Correo electrónico

- Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a Área Logística, a menos que cuente con la autorización del área de T.I.
- Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de Área Logística. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.
- Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

### 3.21 Controles contra virus o software malicioso

- Para prevenir infecciones por virus informático, los usuarios de Área Logística no deben hacer uso de software que no haya sido proporcionado y validado por el área de T.I.
- Los usuarios de Área Logística deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el área de sistemas.
- Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
- Ningún usuario, funcionario , empleado o personal externo, podrá bajar o descargar software de sistemas, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del área de sistemas.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el área de T.I en: Antivirus, Outlook, office, Navegadores u otros programas.
- Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario de Área Logística, distinto al personal del área de T. deberá intentar erradicarlos de las computadoras.

### 3.22 Controles para la Generación y Restauración de Copias de Respaldo (Backups)

- Realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.
- Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.
- Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las

copias de respaldo, debidamente marcadas. Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.

- Las copias de seguridad o Back ups se deben realizar al menos una vez a la semana y el ultimo día hábil del mes. Un funcionario del área de T.I, revisará una vez por semana, el cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

### 3.23 Planes de Contingencia ante Desastre

**PLAN DE CONTINGENCIA**

Son los procedimientos alternativos a la operación normal en la organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo de las operaciones, estando preparándonos para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

a) Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la compañía, ante el evento de un incidente o catástrofe parcial y/o total.

b) El área de T.I debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre.

c) Disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados.

d) Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.

e) Existencia de documentación de los procedimientos manuales a seguir por las distintas áreas usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos.

f) Existencia de documentación de los procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros.

g) Existencia de documentación de pruebas periódicas de la implementación del plan de recuperación ante desastre para verificar tiempos de respuesta, capitalizando los resultados de la pruebas para el afinamiento del plan.

h) Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la compañía.

i) Disponibilidad de copias de respaldo para restablecer las operaciones en las áreas de misión crítica definidas.

### 3.24 Internet

- El acceso a Internet provisto a los usuarios y funcionarios de Área Logística es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por Área Logística, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el área de T.I.
- Los usuarios de Internet de Area Logistica tienen que reportar todos los incidentes de seguridad informática al área de T.I inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que: Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados. Saben que existe la prohibición de descarga de software sin la autorización del área de T.I.
- La utilización de Internet es para el desempeño de sus funciones y cargo en Área Logística y no para propósitos personales.

### 3.25 Acceso Lógico

Cada usuario y funcionario son responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, de su " ID " login de usuario y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de Área Logística, por lo que se deberá mantener de forma confidencial.
El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de Área Logística, debe ser proporcionado por el dueño de la información, el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

**Controles de acceso lógico:**

- Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el área de T.I antes de poder usar la infraestructura tecnológica de Área Logística.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de Área Logística, a menos que se tenga el visto bueno del dueño de la información y del área de T.I.

**Administración de privilegios:**

Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al área de T.I (Administrador de la Red), para el cambio de privilegios.

**Equipo desatendido (Sin contraseñas):**

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el área de T.I cuando no se encuentren en su lugar de trabajo.

**Administración y uso de contraseñas:**

- La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al área de T.I para que se le proporcione una nueva contraseña.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlas.
- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

**Controles para Otorgar, Modificar y Retirar Accesos a Usuarios:**

El área de T.I. es responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.

**Control de accesos remotos:**

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del área de T.I.

### 3.26 Cumplimiento de Seguridad Informática

El área de T.I revisara constantemente el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

- El área de T.I realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.
- El área de T.I podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.
- Los jefes y responsables de los procesos establecidos en Área Logística deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

### 3.27 Violaciones de seguridad Informática

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de T.I.
- Ningún usuario o funcionario de Área Logística debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de T.I.
- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de Area Logística.

### 3.28 Equipos en el Área Administrativa

- La gerencia deberá poner a disposición del área de T.I, la información contractual de los equipos informáticos de Cómputo Escritorio, Portátil y periférica, así como de los servicios de soporte y mantenimiento.
- El área de T.I, será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos.

- El área de T.I, tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación, mismos que serán entregados por la compañía, para los equipos informáticos de cómputo Escritorio, Portátiles y periféricos al momento de la recepción de los mismos.
- Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el Jefe del Área solicitante, los cuales serán evaluados por el área de T.I para su autorización e inclusión en el Plan Anual de Presupuesto correspondiente.
- El área de T.I, es el área encargada de tramitar las asignaciones, reasignaciones, bajas, etc. de equipos informáticos de cómputo Escritorio, Portátiles y periféricos ante la Sección Financiera entidad encargada del Inventario de Activos para su ejecución.
- El grupo de apoyo del área de T.I, elaborará y registrará en cada asignación o movimiento de equipos informáticos de cómputo Escritorio, Portátiles y periféricos, el documento respectivo a dicha solicitud, el cual contiene los datos generales del usuario y de los bienes informáticos entregados, así mismo, contendrá los datos de software instalado autorizado y configuración del equipo, contando con la firma de conformidad del usuario correspondiente.
- Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar al área de T.I el movimiento así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.
- El área de T.I deberá elaborar el pase de salida cuando algún bien informático de cómputo Escritorio, Portátiles y periférico requiera ser trasladado fuera de las instalaciones de Área Logística por motivo de garantía, reparación o evento.
- Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado o a oficinas externas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida quedará a consideración del área de T.I para su autorización y visto bueno.
- Queda prohibida la baja de equipo de cómputo que no cuente con evaluación técnica por parte del área de T.I
- El área de T.I no es responsable de proporcionar asesoría técnica, mantenimiento preventivo o correctivo a equipo de cómputo propiedad del usuario.
- El usuario que ingrese equipos de su propiedad a las instalaciones de Área Logística es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad del área de T.I.
- Queda prohibido instalar software no autorizado o que no cuente con licencia, el área de T.I deberá realizar las instalaciones de acuerdo con los estándares de Área Logística.
- Es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en la misma.

- El área de T.I no es responsable de la configuración de dispositivos personales tales como Palms, iPOD y teléfonos celulares propiedad del usuario.
- El usuario que requiera la instalación de Software de su propiedad deberá solicitar por escrito al área de T.I anexando copia de la licencia que compruebe su propiedad o en el caso de software libre el documento probatorio.

## 4. DEFINICIONES

**4.1** **T.I.**: Tecnologías de la información.

## 5. REFERENCIAS

**5.1** ISO 27000 “Seguridad de la información”.

## 6. ANEXOS

**6.1** FR-MC 01 Encuesta de satisfacción de clientes

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| Firma: **Cristina López** | Firma: **Mònica Martìnez P** | Firma: **John Jairo Álvarez** |
| **Nombre:** Cristina Lopez | **Nombre:** Mònica Martìnez | **Nombre:** John Jairo Alvarez |
| **Fecha:** 05/07/2013 | **Fecha:** 05/07/2013 | **Fecha:** 05/07/2013 |