## A. POLÌTICAS DE PROTECCIÒN Y SEGURIDAD DEL SOFTWARE

- Solo se podrá utilizar en los equipos de la empresa, el software autorizado por la Gerencia, instalado en el disco duro del equipo. No se deben ejecutar en los equipos programas que se traigan de CD's, memorias, discos o cualquier medio de almacenamiento ya que estas licencias no están registradas y se consideran ilegales.
- Todos los dispositivos de almacenamiento, tales como , CD's, Memorias USB, y todo lo que implique conectividad al equipo por el puerto USB, deberá ser revisado previamente por el departamento Sistemas, o en su defecto revisado por el antivirus con el fin de evitar el ingreso de virus que puedan afectar el buen funcionamiento de la red de la compañía.
- Cualquier adición o remoción de software de los equipos solo podrá ser coordinada y realizada por personal autorizado de Sistemas.
- No se podrá instalar aplicaciones que degraden el rendimiento, confiabilidad, disponibilidad y/o estabilidad del funcionamiento de los equipos.

## B. POLÍTICAS DE PROTECCIÒN Y SEGURIDAD DE LOS EQUIPOS

- Todo funcionario es responsable por la custodia y manejo de los computadores, impresoras u otros equipos que se encuentren asignados a su cargo, y su responsabilidad se extiende a los daños ocasionados a estos dispositivos por el uso indebido siempre que los daños se deban a negligencia o descuido en la operación.
- En caso de detectarse cualquier tipo de falla en el equipo reportar inmediatamente al departamento de sistemas dejando registro en http://soporte.valleygroups.com/
- Es responsabilidad de cada empleado apagar los equipos, de oficina que estén a su cargo al finalizar la jornada diaria de trabajo.
- Los usuarios no deben abrir los computadores, impresoras, módem, reguladores de voltaje u otros equipos, para retirar, sustituir, reparar o instalar partes.
- Se prohíbe el consumo de alimentos en zonas de instalación de equipos de cómputo. En caso de que el equipo sufra algún daño, por derrame de líquidos, será cobrado al empleado responsable.
- No se deben colocar elementos tales como plantas, alimentos o líquidos sobre los equipos ni bloquear sus rejillas de ventilación con papeles u otros objetos.
- En los multitomas de color **naranja** que proveen corriente regulada (UPS) destinados a alimentar eléctricamente los equipos de cómputo, no deben ser conectados equipos diferentes como ventiladores, aspiradoras, cargadores, etc.
- Para retirar equipos de cómputo o cualquier otro activo de las instalaciones de la compañía, debe reportar este retiro al departamento de sistemas quien en documento asignado para esto dara autorización.
- Para los equipos portátiles se debe hacer buen uso de las baterías, utilizando los ciclos completos de carga y descarga.
- Para los equipos portátiles se prohíbe el llevarlos a mantenimiento correctivo o preventivo a negocios o terceros no autorizados por el departamento de sistemas.
- Se prohíbe ceder, vender, alquilar los equipos de cómputos fijos o portátiles, asignados para su labor.
- En caso de sufrir robo o hurto del equipo portátil deberá reportar inmediatamente al departamento de sistemas con un documento escrito donde se redacten los hechos mencionando modo tiempo y lugar, información que será entregada al

corredor de seguros quien le indicara como instaurar la denuncia. El denuncio ante las autoridades competentes solo podrá ser realizado previa autorización e indicaciones dadas por el jefe de sistemas,. Después de colocado el denuncio este debe ser entregado en original al departamento de sistemas. La empresa reportara el robo o pérdida del equipo a la compañía aseguradora para iniciar los trámites de reclamación. El deducible cobrado por la compañía de seguros debe ser asumido por el empleado, excepto cuando el hurto sea mediante sustracción forzada.
Si la pedida del equipo se ocasiona incumpliendo las políticas de retiro de los bienes de la empresa la responsabilidad de la pérdida tanto del valor del equipo o deducible es a cargo 100% por el empleado

## C. POLÍTICAS SOBRE CONFIDENCIALIDAD Y PROTECCIÒN DE LA INFORMACIÒN.

- Todo usuario se debe comprometer a mantener reserva y a no divulgar información confidencial ni datos relacionados con los negocios de la empresa, productos, servicios, clientes, sistemas, planes de negocio, estrategias de mercado u otras informaciones confidenciales.
- La clave personal que permite la consulta / ejecución de transacciones automáticas, ingresos a programas como CGUNO , es de uso privado y personal y bajo ninguna circunstancia debe ser entregada o dada a conocer a otra persona, en caso de un reemplazo se debe solicitar a la persona encargada de administrar el sistema, la clave y autorizaciones provisionales correspondientes para ingresar a la aplicación, teniendo especial cuidado que siempre que se ingrese, esta no sea observada por otra persona.
- La clave debe ser definida en forma que no sea fácilmente deducible. Se debe evitar el uso de nombres personales, números de cédula, placas de carros, fechas de cumpleaños y otras palabras que se relacionen con hechos y datos de fácil obtención.
- Cuando un usuario deba retirarse del sitio de trabajo ya sea temporal o al terminar su labor diaria, deberá desactivarse su clave de acceso (salirse del sistema).
- El manejo de las claves, implica responsabilidades sobre su uso, el cual se extiende hasta la protección de información contra accesos no autorizados.
- Se debe crear una carpeta en la unidad C, denominada DOCUMENTOS, para guardar en esta, todos los archivos necesarios para la labor diaria y que ameriten tener un respaldo de backup. Los documentos que no estén incluidos en esta carpeta, no contarán con copia de seguridad.
- Es responsabilidad del usuario poner a disposición su equipo para la realización del backup semanal, es decir dejar los equipos encendidos en los días indicados a través de comunicación interna por medio del correo.
- El correo electrónico enviado en forma privada a cada usuario, no debe ser interferido o leído por otros usuarios, así como tampoco utilizar este medio con fines fraudulentos, o enviar mensajes obscenos ni destructivos a otros usuarios.
- Depurar constante el correo electrónico para no tener inconvenientes de pérdida de información y que no se pueda abrir la aplicación por los tamaños de los archivos, y no olvidar vaciar la carpeta de eliminados.

## D. POLITICAS SOBRE USO DE HERRAMIENTAS DE COMUNICACIÓN INTERNA

- el acceso a Internet ES MONITOREADO , este es solo para accesar a paginas que tengan relación con sus funciones, está terminantemente prohibido el ingreso a las redes sociales, correos personales, chat, descarga de archivos, video y música en línea, las líneas telefónicas y todos los recursos necesarios para establecer interconexión entre las diferentes redes de la empresa son limitados y costosos, prohibido el uso inadecuado y exagerado de chat y correos en equipos Black Berry o de tecnología de plan de datos de uso personal, en horas laborales **.**
- La herramienta de Mensajería instantánea (Spark) es una plataforma de comunicación interna y por lo tanto únicamente para uso laboral y no para tratar temas personales. Si usted va a insertarle foto a su usuario del Spark, debe ser foto documento (tipo carnet )
- Los empleados que tengan Black Berry dentro del plan corporativo, la foto del perfil debe ser la imagen corporativa de Valley Groups. La imagen del escritorio de los equipos de cómputo debe ser la corporativa sin excepción alguna.

| ELABORADO POR | REVISADO POR | APROBADO POR |
|---|---|---|
| Nombre: Gilmer Betancourth | Nombre: Jhon H. Cortes B. | Nombre: Jaime Cortes W. |
| Cargo: Jefe de Sistemas | Cargo: Jefe del SIG | Cargo: Vicepresidente Administrativo |
| Firma | Firma | Firma |