

	VICTORIA CARGO TRANSPORTES SAS			
	POLITICA DE SEGURIDAD INFORMATICA			
	CÓDIGO: GA-OD-05-V02	F. EMISIÓN: Agosto 2009	F. REVISIÓN: Noviembre 2011	PAGINACIÓN Página 1 de 1

Con el fin de preservar los sistemas de información y asegurar que estas no sean objeto de fraude o sustracción de los mismos se establecieron las siguientes políticas de seguridad informática:

1. La contraseña de acceso de los equipos deberá cambiarse al menos una vez cada mes y el sistema deberá exigir dicho cambio basado en las siguientes características:
 - Contiene siete caracteres mínimos.
 - No se ha usado en al menos 24 ocasiones.
 - No se cambio dentro del último día.
 - No contiene su cuenta o nombre completo.
 - Contiene al menos tres de los siguientes cuatro grupos de caracteres: mayúsculas, minúsculas, números y caracteres no alfabéticos.
2. Cada equipo se encuentra denominado con el nombre de usuario de la persona o el cargo que ocupa y este es el Responsable del manejo del mismo.
3. El Back up de los equipos de computo de cada usuario se encuentran almacenados en el disco duro extraíble conectado al servidor de la oficina Principal. El back up se realiza diariamente a las 12:00 p.m. de manera automática, al igual que lo realiza también del Software Contable, del Software de Transporte y de la carpeta Común que se encuentra en el Servidor.
4. El Back up de la información del Sistema de Información Contable está a cargo de la Directora Financiera y de la contadora, quienes cada semana exportan el back up que es generado automáticamente por el servidor en una memoria extraíble y lo custodian.
5. El Back up general de la compañía está a cargo de la Directora Administrativa quien cada semana retira la cinta RD1000 DATA CARTRIDGE y lo custodia. Este back up se realiza diariamente a la 1 a.m. exportando las siguientes carpetas: Común, usuarios, CG UNO, Simanca.
6. A fin de evitar ataques de virus, la Compañía ha dispuesto un Firewall que administra el internet de la Organización, restringiendo en los usuarios el acceso a páginas de ocio, tales como: música, videos, descargas de juegos y software. De la misma manera se cuenta con una licencia de antivirus el cual está configurado para realizar actualizaciones automáticas.
7. El Mantenimiento preventivo y de limpieza a los equipos de cómputo y los equipos de oficina en general deberá realizarse mínimo dos veces en el año.

En caso de detectar incumplimiento a la política de seguridad informática definida por la Compañía que ocasionen daños graves a los sistemas y a los datos comerciales se le impondrán medidas disciplinarias tales como llamados de atención y suspensión si es el caso.