	POLITICA DE SEGURIDAD INFORMATICA	Código: P GT 001
		Fecha: 21 05 2016
		Versión: 04
		Página 1 de 6

1. OBJETIVO

Establecer la política de seguridad informática para garantizar la seguridad de la información.

2. ALCANCE

Esta Política debe ser aplicada por todos los procesos (Misionales, Dirección y Apoyo), usuarios de Tecnología Informática.

3. DEFINICIONES


- 3.1 Política de Seguridad Informática:** Directriz que conduce a garantizar la seguridad informática
- 3.2 Servidor:** Computador con características técnicas especiales, donde se administran los archivos y periféricos de una red.
- 3.3 Red:** Conjunto de Computadores de una Empresa, donde se comparte información y Recursos.
- 3.4 Switch:** Dispositivo donde van conectados cada uno de los puntos de red de un Empresa.
- 3.5 Servidor Proxy:** Computador encargado de Administrar el Uso del Internet en la Empresa.
- 3.6 Personal de la Empresa:** Personal cuyo cargo figure en el organigrama empresarial.
- 3.7 Personal Externo:** Usuarios ocasionales (visitantes, clientes, proveedores).

4. RESPONSABILIDADES

No	Actividad	Responsable
1	Seguridad De Redes	Líder Tics
2	Seguridad Eléctrica	Líder Tics
3	Seguridad Área De Servidores	Líder Tics
4	Seguridad Internet Y Correo	Líder Tics
5	Seguridad Programas Y Aplicaciones	Líder Tics
6	Seguridad Equipos De Computo	Líder Tics
7	Seguridad De La Información	Líder Tics

5. POLITICAS Y CONDICIONES

- 5.1 Política de Seguridad Informática:** Garantizar la seguridad de la información a través de mecanismos de control que permitan la utilización adecuada de los recursos tecnológicos e informáticos de la empresa
- 5.2** Todo el personal de la Empresa, está en la obligación de comunicar al líder Tics toda causa de posibles problemas en el sistema informático a fin de tomar acciones preventivas pertinentes igualmente debe quedar registro en el Formato F GT 010 Formato Solicitud de Servicios Técnicos.

	<p align="center">POLITICA DE SEGURIDAD INFORMATICA</p>	Código: P GT 001
		Fecha: 21 05 2016
		Versión: 04
		Página 2 de 6

- 5.3** Todo el personal de la empresa debe dar cumplimiento a este procedimiento el cual es divulgado en la inducción corporativa o cuando se presentan cambios o actualizaciones del mismo.
- 5.4** El Líder de Tics, tiene el control y archivo adecuado e identificable de todo el Software Licenciado en el Formato F GT 007 Listado De Licencias de Software, y el Hardware relacionados en el Formato F GT 006 Inventario de Activos de la Empresa.
- 5.5** Un Servidor Firewall administra la seguridad y el acceso a Internet mediante políticas administrativas, donde los usuarios no tienen acceso a Redes Sociales, Correos Públicos, sitios web de contenido para adultos y otros de diversión como música y videos. Por lo tanto, a cada funcionario que intente ingresar a cualquiera de éstas páginas le será impuesto un llamado de atención con copia a la hoja de vida.

6. DESARROLLO

6.1. Seguridad De Redes

6.1.1. Oficina Principal

Para garantizar el Buen Servicio y Seguridad de Red, la Empresa cuenta con cableado estructurado UTP categoría 6 con velocidad de transmisión de 1 Gb/s, cuyas características técnicas garantizan la comunicación efectiva entre los puntos de red del Switch y los Puntos de Red de cada usuario.

Transportes Centro valle cuenta con Equipos tecnológicos como Switch y Strip telefónicos, los cuales permiten la comunicación técnica adecuada a cada uno de los Usuarios de los Equipos de Cómputo y líneas telefónicas análogas. Estos elementos están instalados adecuadamente en dispositivos denominados Rack, los cuales están ubicados en la Sede Principal y Oficinas de la Empresa.


6.1.2. Software - Accesibilidad

El sistema informático de la empresa cuenta con un software que valida el ingreso al dominio a través de claves, estas claves son asignadas por el Líder de Tics a usuarios de la empresa.

Las claves asignadas a SIESA no pueden ser transferidas, el Sistema Contable SIESA, cuenta con un sistema de auditoría que registra todos los accesos y modificaciones a las bases de datos es importante tener en cuenta que la manipulación de la estructura de tablas solo la debe ser el proveedor.

Todo permiso asignado a SIESA, debe ser autorizado por los líderes de proceso. El Lider TICS debe registrarlos en el formato F GT 010 Solicitud de Servicios Técnicos.

Las claves deben ser cambiadas cada 180 días tanto del Acceso al Dominio de la Empresa y de 90 días al Programa Contable.

	POLITICA DE SEGURIDAD INFORMATICA	Código: P GT 001
		Fecha: 21 05 2016
		Versión: 04
		Página 3 de 6

6.2. Seguridad Eléctrica

Transportes Centro Valle cuenta con el respaldo de una Planta Eléctrica que garantiza la fluidez continua de electricidad en caso de corte. Esta Planta funciona después de 1 minuto del corte eléctrico y durante ese lapso tenemos el soporte de una U.P.S. on line de 5 KVA

Por ningún motivo se deben conectar las Impresoras Láser ni ningún otro aparato eléctrico o electrónico diferente a los Equipos de Computación igualmente dispositivos como cargadores, electrodomésticos, etc.

Descripción de los Equipos de Protección Eléctrica:

SEDE	DISPOSITIVO
Buenaventura	1 Planta Eléctrica 2.5 KVA Honda 1 UPS de 1500 VA
Bogotá	Conectado al fluido eléctrico del Centro Comercial Montevideo
Barranquilla	1 UPS APC 550 VA
Principal	UPS 5 KVA ONLINE Planta eléctrica 50 KVA trifásica Enermax
Ingredion	Sistemas regulado y protegido de Ingredion
Buga	Regulador de voltaje de 300 VA.

6.3. Seguridad Área De Servidores


El Área del servidor esta climatizada con temperatura que va en un rango de 10° centígrados a 20° centígrados.

La Empresa tiene como política que el manejo del servidor es restringido y el acceso al mismo será permitido al Líder de Tics, o personal que se autorice bajo supervisión permanente.

6.4. Seguridad Internet y Correo

La Empresa cuenta con los servicios de Internet, telefonía Fija y Celular los cuales han sido contratados con proveedores confiables, estos servicios de comunicación tienen los mecanismos de seguridad adecuados. El líder TICS se encarga de la administración, supervisión y control, para realizar la prestación adecuada de los servicios de comunicación tanto interna como externa.

En Transportes Centro Valle la seguridad de red es hoy una cuestión prioritaria ya que se garantiza la seguridad de la información a través de mecanismos de control como el sistema Firewall FORTINET Firmware Versión v5.2.4, build688, el cual posee una política integradora, aglutinando y combinando características y funciones que administran la seguridad y el acceso a Internet mediante políticas administrativas donde los usuarios no tienen acceso a Redes Sociales, FaceBook, Correos Públicos, sitios web de contenido para adultos y otros de diversión como música y videos.

	POLITICA DE SEGURIDAD INFORMATICA	Código: P GT 001
		Fecha: 21 05 2016
		Versión: 04
		Página 4 de 6

Esto permite la optimización de los tiempos laborados por los colaboradores, evitando posibles distracciones y permitiendo de esta manera la utilización adecuada de los recursos tecnológicos e informáticos de la empresa.

6.5. Acceso a personal externo

Se concederá el acceso a Internet al personal externo de Transportes Centrovale por medio de WI-FI o por medio de acceso mediante red cableada (Ethernet), el personal externo no tendrá acceso a los archivos almacenados en Compartidos y Usuarios, para esto se utiliza la seguridad que brinda el firewall.

Si una persona externa llegase a necesitar un archivo de Compartidos y/o Usuarios o acceso al sistema contable, deberá hacerlo desde un computador de la empresa con autorización y siendo acompañado por un empleado de Transportes Centrovale.

La clave de la red inalámbrica deberá ser solicitada al líder Tic's. el cual la configurara en el equipo del usuario externo y realizara los ajustes correspondientes.

Transportes Centrovale no se hará responsable por sanciones o multas debido a software no licenciado que esté Instalado en los computadores del personal externo.

6.6. Programas y Aplicaciones

Todos los Programas y Aplicaciones de Informática cuentan con su licencia de uso, Estas licencias están almacenadas en un Lugar Seguro, donde solo el Líder de Tics o alguien delegado y supervisado acceden a estas licencias.


Está prohibido el uso de programas que no cuenten con dichas licencias. Los Equipos poseen restricciones para que un Usuario no pueda instalar dicho Software.

6.7. Equipos De Computo

Todo Usuario es responsable del uso y cuidado de los equipos de cómputo y del acceso al sistema.

6.8. Seguridad contra virus y amenazas

La empresa cuenta con un antivirus KASPERSKY ENDPOINT SECURITY 10 FOR WINDOWS VERSION 10.2.4.674 (mr2) el cual está instalado en todos los equipos, este antivirus brinda protección frente a virus y amenazas, está configurado de manera que reciba actualizaciones automáticas del fabricante diariamente.

	POLITICA DE SEGURIDAD INFORMATICA	Código: P GT 001
		Fecha: 21 05 2016
		Versión: 04
		Página 5 de 6

6.9. Seguridad De La Información

Con el fin de tener un respaldo de la información de la empresa en caso de deterioro o pérdida de la misma se tienen en cuenta las siguientes medidas de seguridad

6.9.1. Respaldo De Garantías

Todo el Software de la empresa como SIESA ENTERPRISE, NOMINA WEB, OFFICE 365, OFFICE 2010, OFFICE 2013, WINDOWS 7 PROFESIONAL, WINDOWS 10, WINDOWS 2008 R2, WINDOWS 2012 R2, SQL, cuenta con el respaldo de Garantía por parte de los proveedores y los medios necesarios en caso de pérdida o daño del mismo.

6.9.2. Control de Accesos


La carpeta donde reside la información del Sistema Integrado de gestión de Calidad (SGC-TCV) tiene control de acceso sobre las subcarpetas según esta establecido en el registro F GT 011 Control de acceso de información medio magnético.

Este control se realiza utilizando las listas de control de acceso (ACL) de Windows Server 2012.

6.9.3. Respaldo de Información

Se realiza el backup de información del Programa Contable, Carpeta usuarios y Compartidos y Correos Electrónicos de acuerdo al Instructivo I GT 003 Instructivo para realizar Copias de Seguridad.

Tipo de Datos o Aplicativo	Periodicidad del Backup	Tipo del backup	Medio de Almacenamiento	Lugar de Almacenamiento	Quien Genera
Sistemas Contable Histórico y Nuevo.	Diario	Disco Duro Interno	Disco Duro Interno	Servidor Neptuno	Líder Tic`s
BD, Datos de Usuarios y Compartidos	Diario	Disco Duro Interno.	Disco Duro Interno.	Servidor Neptuno	Líder Tic`s
Siesa, BD y Datos de Usuarios	Semanal (Lunes y Viernes)	En caso de Siniestro	Disco Duro Externo	Servidor Neptuno	Líder Tic`s
Siesa	Mensual	Histórico	Disco Duro Interno	Caja fuerte	Líder Tic`s
Correo Electrónico	Trimestral	Disco Duro Externo	Disco Duro Externo	Caja Fuerte	Usuarios de Correo.

	POLITICA DE SEGURIDAD INFORMATICA	Código: P GT 001
		Fecha: 21 05 2016
		Versión: 04
		Página 6 de 6

7. DIAGRAMA DE FLUJO

N/A.

8. DOCUMENTOS Y REGISTROS RELACIONADOS

No	Código	Documento/Registro	Localización	Responsable
1	F GT 006	Inventario de Activos de la Empresa	Compartidos/ Calidad/ Tics / Registros	Líder Tic's
2	F GT 007	Listado De Licencias de Software	Compartidos/ Calidad/ Tics / Registros	Líder Tic's
3	F GT 010	Formato Solicitud de Servicios Técnicos	Compartidos/ Calidad/ Tics / Registros	Líder Tic's
4	F GT 011	Control de acceso de información medio magnético	Compartidos/ Calidad/ Tics / Registros	Líder Tic's
5	I GT 003	Instructivo para realizar Copias de Seguridad.	Compartidos/ Calidad/ Tics / Instructivos	Líder Tic's

9. CONTROL DE APROBACIÓN DEL DOCUMENTO

Elaborado Por	Revisado Por	Revisado Por	Aprobado Por
Líder Tic's	Líder de Gestión de Calidad y Medio Ambiente	Representante de la Dirección	Gerente General
Fecha: 21 05 2016	Fecha: 21 05 2016	Fecha: 21 05 2016	Fecha: 21 05 2016
			