


| | | |
|---|--|-------------------|
|  | POLITICA DE SEGURIDAD INFORMATICA | Código: P GT 001 |
| | | Fecha: 12 09 2012 |
| | | Versión: 02 |
| | | Página 1 de 5 |

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 por escrito a través del Formato F GT 010 Formato Solicitud de Servicios Técnicos, al Líder de Tics, toda causa de posibles problemas en el sistema informático a fin de tomar acciones preventivas pertinentes.

| | | |
|---|--|-------------------|
|  | POLITICA DE SEGURIDAD INFORMATICA | Código: P GT 001 |
| | | Fecha: 12 09 2012 |
| | | Versión: 02 |
| | | Página 2 de 5 |

- 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.

6. DESARROLLO

6.1. Seguridad De Redes

6.1.1. Hardware

Para garantizar el Buen Servicio y Seguridad de Red, la Empresa cuenta con una tendida de cableado estructurado, cuyas características técnicas garantizan la comunicación efectiva entre los puntos de red del Switch y los Puntos de Red de cada usuario. Utilizando la más alta gama de material para este tendido como es la categoría 6 del cable U.T.P.

Cuenta con Equipos tecnológicos como Switch y Script telefónicos, los cuales permiten la comunicación técnica adecuada a cada uno de los Usuarios de los Equipos de Cómputo y líneas telefónicas. Estos elementos están instalados adecuadamente en dispositivos denominados Rack. Estos Rack 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 Novasoft no pueden ser transferidas, el Novasoft cuenta con un sistema de auditoría que registra todos los accesos y modificaciones a las bases de datos.


Todo permiso es autorizado utilizando el formato F GT 010 Solicitud de Servicios Técnicos, por los Líderes de Procesos, donde se le da el perfil al Usuario.

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

6.2. Seguridad Eléctrica

Todos los Equipos cuentan con alimentadores eléctricos, que se conectaran a la Red Eléctrica Exclusiva para equipos de Cómputo. Se cuenta con una U.P.S que da un respaldo al momento de un corte de Electricidad y una Planta Eléctrica que respalde cualquier contingencia de corte del Fluido Eléctrico.

No se debe conectar en la toma corriente de las U.P.S. las Impresoras Láser ni ningún otro aparato eléctrico o electrónico diferente a los Equipos de Computación.

| | | |
|---|--|-------------------|
|  | POLITICA DE SEGURIDAD INFORMATICA | Código: P GT 001 |
| | | Fecha: 12 09 2012 |
| | | Versión: 02 |
| | | Página 3 de 5 |

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 Subcontrata con proveedores confiables los servicios de comunicaciones como Internet y telefonía Fija y Celular, quienes establecen los mecanismos de seguridad adecuados. La supervisión de la prestación adecuada del servicio, así como de todo lo relacionado a la comunicación externa es responsabilidad del Líder de Tics.

Los permisos de navegación en internet serán implementados por el Proceso de Tics. Se cuenta con un Servidor Proxy y firewall el cual administra y maneja la seguridad del uso del Internet a través de programas de Restricciones donde los usuarios no tendrán acceso a Redes Sociales, Correos Públicos y en fin cualquier tipo de información que no tenga que ver con el normal desarrollo de los Procesos de la empresa.

Todos los Usuarios deberán tener una cuenta de correo electrónico provista por el Proceso de Tics.

6.5. Acceso a personal externo

Se concederá el acceso a Internet al personal externo de Transportes Centrovalle 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 Hércules, para esto se utiliza la seguridad que brinda Windows Server 2003 por medio de ACL (Access control list).

Si una persona externa llegase a necesitar un archivo de Hércules o acceso al aplicativo empresarial, deberá hacerlo desde un computador de la empresa con autorización y siendo acompañado por un empleado de Transportes Centrovalle.


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 Centrovalle 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.

| | | |
|---|--|-------------------|
|  | POLITICA DE SEGURIDAD INFORMATICA | Código: P GT 001 |
| | | Fecha: 12 09 2012 |
| | | Versión: 02 |
| | | Página 4 de 5 |

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 el cual está instalado en todos los equipos, este antivirus brinda protección frente a virus y amenazas, está configurado de manera que reciba actualizaciones del fabricante diariamente.

6.8. 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

6.8.1. Respaldo De Garantías

Todo el Software de la empresa cuenta con el respaldo de Garantía por parte de los proveedores en caso de pérdida o daño del mismo. Se cuenta con el código fuente que nos permita la recuperación de la aplicación.

6.8.2. Control de Accesos

La carpeta donde reside la información del sistema 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 2003.

6.8.3. Backup 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.


7. DIAGRAMA DE FLUJO

7.1. 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 | Compartidos/ Calidad/ | Líder Tic's |

Este documento es de propiedad intelectual de TRANSPORTES CENTRO VALLE S.A. y no puede ser reproducido o utilizado sin previa autorización.

| | | |
|---|--|-------------------|
|  | POLITICA DE SEGURIDAD INFORMATICA | Código: P GT 001 |
| | | Fecha: 12 09 2012 |
| | | Versión: 02 |
| | | Página 5 de 5 |

| No | Código | Documento/Registro | Localización | Responsable |
|----|----------|--|---|-------------|
| | | información medio magnético | Tics / Registros | |
| 5 | I GT 003 | Instructivo para realizar Copias de Seguridad. | Compartidos/ Calidad/ Tics / Instructivos | Líder Tic's |

9. CONTROL DE MODIFICACIONES

| No | Fecha | Naturaleza del Cambio | Versión |
|----|------------|---|---------|
| 1 | 03/01/2011 | Primera Emisión del documento | 1 |
| 2 | 12/09/2012 | Se incluye definición de personal de la Empresa y Personal Externo y se en el punto 6.5 se define política de Acceso a personal Externo y se incluye el F GT 011, Control de acceso de información medio magnético. | 2 |
| 3 | | | 3 |
| 4 | | | 4 |

10. 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: 12 09 2012 | Fecha: 12 09 2012 | Fecha: 12 09 2012 | Fecha: 12 09 2012 |
|  |  |  |  |