

**POLÍTICA DE SEGURIDAD DE TIC’S**

PROCESO GESTIÓN DE TIC’S

GLT-GT-DOC-01

Versión 1

Edición: Febrero 15 de 2014

|  |  |  |
| --- | --- | --- |
| **Elaborado Por:**  Director TICS | **Revisado Por:**  Representante Alta Dirección | **Aprobado Por:**  Gerente General Galotrans |
| **Camilo Garavito** | **Ana María Garavito** | **Alonso Garavito** |
| **Fecha:** 31-Ene- 2013 | **Fecha:** 15- Feb- 2014 | **Fecha:** 15- Feb- 2014 |

**Control de Cambios**

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha Modificación** | **Comentario – Justificación** |
| 1 | 15-Feb-14 | Versión inicial |
|  |  |  |
|  |  |  |
|  |  |  |

TABLA DE CONTENIDO

[1 Objetivo 4](#_Toc380505469)

[2 Alcance 4](#_Toc380505470)

[3 Definiciones 4](#_Toc380505471)

[4 Niveles De Seguridad 5](#_Toc380505472)

[4.1 Nivel 1: Seguridad Organizacional 5](#_Toc380505473)

[4.1.1 Políticas De Seguridad 5](#_Toc380505474)

[4.1.2 Excepciones De Responsabilidad 6](#_Toc380505475)

[4.1.3 Clasificación Y Control De Activos. 6](#_Toc380505476)

[4.1.4 Seguridad Ligada Al Personal 6](#_Toc380505477)

[4.2 Nivel 2: Seguridad Lógica 7](#_Toc380505478)

[4.2.1 Control De Acceso 7](#_Toc380505479)

[4.2.2 Gestión De Operaciones 10](#_Toc380505480)

[4.3 Nivel De Seguridad Física 11](#_Toc380505481)

[4.3.1 Resguardo De Los Equipos De Tecnología 11](#_Toc380505482)

[4.3.2 Controles Físicos Generales 11](#_Toc380505483)

[4.3.3 Actividades Prohibidas 11](#_Toc380505484)

[4.4 Seguridad Legal 11](#_Toc380505485)

[4.4.1 Cumplimiento De Requisitos Legales 11](#_Toc380505486)

# OBJETIVO

Preservar la integridad, disponibilidad y confidencialidad de la información, mediante el empleo y correcto funcionamiento de las políticas y normas de seguridad tecnológicas con base en la gestión del riesgo; con el fin de proteger el hardware y software de Galotrans S.A, así como toda la información procesada y almacenada en los mismos.

# ALCANCE

El ámbito de aplicación del manual de normas y políticas de seguridad informática, se aplica a todo el personal vinculado a Galotrans S.A que haga uso de la infraestructura tecnológica en alguna de sus tres sedes, compuesta por los servicios de hardware y software.

# DEFINICIONES

* **TICS:** Tecnologías de la información y comunicación.
* **Administradores de tecnología:** Se denominan administradores de tecnología las personas pertenecientes al proceso de TIC’s.
* **Archivo Log:** Ficheros de registro o bitácoras de los sistemas, en los que se recoge información de sucesos, alertas, errores, eventos de conexiones, IP’s, e información de la actividad del usuario en el sistema.
* **Ataque:** Evento, exitoso o no, que busca atentar contra el buen funcionamiento del sistema.
* **Cuenta:** Mecanismo de identificación del usuario en el sistema, el cual le permite autenticarse y obtener privilegios sobre el mismo.
* **Contingencia:** Plan alterno que permite mitigar un riesgo generado sobre la disponibilidad de la información o procesamiento de la misma en la infraestructura de sistemas.
* **Cifrar:** Proceso mediante el cual se procesa información con base en un modelo, para ocultar el mensaje de agentes no autorizados.
* **Disponibilidad:** Accesibilidad a la información cuando ésta sea solicitada.
* **Integridad:** Proteger la información de alteraciones no autorizadas por la organización.
* **Impacto:** Consecuencia de la materialización de una amenaza.
* **Normativa de Seguridad ISO/27001:2013:** El Sistema de Gestión de Seguridad de la información es un conjunto de buenas prácticas y lineamientos que ofrece ISO.
* **Red Empresarial:** Conectividad de los equipos y dispositivos a la red alámbrica o inalámbrica que ofrece un servicio empresarial, ya sea internet, servicios compartidos, acceso aplicaciones, etc.
* **Responsabilidad:** Se denomina responsable directo, al individuo de la empresa que debe mantener seguros los activos de cómputo e información correspondientes.
* **Usuario:** Se define como cualquier persona natural o jurídica que utilice los recursos tecnológicos de Galotrans S.A y tenga una vinculación con la empresa.
* **Vulnerabilidad:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

# NIVELES DE SEGURIDAD

Los niveles de seguridad fueron desarrollados con base en el esquema normativo de seguridad ISO 27001:2013, donde se resaltan el conjunto de buenas prácticas aplicables con base en el lineamiento de la Alta Gerencia y las necesidades del negocio. En las políticas se describe con cautela qué activo proteger, de que protegerlo, cómo protegerlo y por qué protegerlo.

## Nivel 1: Seguridad Organizacional

### Políticas de seguridad

* Los servicios de red empresarial son de exclusivo uso laboral, de investigación y para gestiones operacionales o administrativas; cualquier cambio en la normativa de los mismos, será expresa y adecuada como política de seguridad en este documento.
* La Alta Dirección de Galotrans S.A delegará al proceso de Gestión de TIC’s el seguimiento al cumplimiento de la normativa, para que propicie el entorno necesario para crear un SGSI de una manera incremental a través del tiempo, el cual tendrá entre sus funciones:
  + Velar por la seguridad de los activos informáticos.
  + Gestión y procesamiento de información.
  + Cumplimiento de Políticas.
  + Elaboración de planes de seguridad.
  + Capacitación de usuarios en temas de seguridad.
  + Gestionar y coordinar esfuerzos, para crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de la empresa. El mismo guiará a los empleados, la forma o métodos necesarios para salir adelante ante cualquier eventualidad que se presente.
  + El director de TIC’s es el encargado de asegurar y mantener en buen estado los servidores dentro de la red empresarial.
  + Todo usuario de la red empresarial de Galotrans S.A. gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red, sus servicios o cualquier otra red ajena a la empresarial. Los administradores de tecnología podrán solicitar los datos de usuario y contraseña para las respectivas validaciones de inconvenientes sobre los sistemas.
  + Los usuarios tendrán acceso a internet de acuerdo a las dinámicas laborales inherentes a sus cargos. El control de contenido (según dado el caso) se realizará restrictivamente de acuerdo a la evaluación de seguridad del Proceso de TIC’s y posterior aprobación de la Alta Dirección.

### Excepciones de Responsabilidad

* Los usuarios que por disposición de sus superiores realicen acciones que perjudiquen a otros usuarios o la información que estos procesan, y si estos no cuentan con un contrato de confidencialidad y protección de la información de la empresa o sus allegados.
* Algunos usuarios pueden estar exentos de seguir algunas de las políticas enumeradas en este documento, debido a la responsabilidad de su cargo, o a situaciones no programadas. Estas excepciones deberán ser solicitadas y aprobadas por la Alta Dirección, y supervisadas por el Proceso de TIC’s.

### Clasificación y control de activos.

#### Responsabilidad por los activos

* Cada empleado directo al que se le haya asignado uno o varios activos de la empresa, es el único responsable y debe velar por el correcto cuidado y funcionamiento. Además, de salvaguardar cualquier activo: físico, de software y de información contenida en los mismos.
* Los administradores de tecnología son los responsables de la seguridad de la información almacenada en esos recursos y de los BackUp (GLT-GT-DOC-02) realizados por cada uno de los trabajadores de la compañía.

#### Clasificación de la información

### Seguridad ligada al personal

#### Contratos

Se anexará al contrato la aceptación del documento de Política de Confidencialidad, en el cual se expresa la responsabilidad de cualquier empleado de Galotrans en el manejo adecuado de la información y cualquier activo o propiedad intelectual de la empresa.

#### Empleado

* Toda la información manipulada, procesada o almacenada por el empleado es propiedad exclusiva de Galotrans.
* Galotrans no se hace responsable por cualquier tipo de perjuicio causado por alguno de sus empleados a la información o dispositivos de procesamiento, propiedad de la empresa.
* Galotrans no se hace responsable por cualquier uso inadecuado o indebido de los recursos de tecnología por parte de los empleados que perjudiquen a cualquier ente externo, organización, norma o legislación.

#### Capacitación de usuarios

* Los empleados de Galotrans serán capacitados en los temas referentes a seguridad de la información, políticas de seguridad, etc, de acuerdo a las actividades que cada uno desempeña en los cargos asignados. Se dejará constancia física de dicha capacitación con la firma del empleado, fecha, hora y temas tratados. Esta evidencia se adjuntará al expediente de formación del proceso de RH.

#### Atención a Incidentes y anomalías de seguridad

* Se realizarán respaldos de la información para los activos de mayor importancia o críticos diariamente, un respaldo semanal que se utilizar en caso de fallas y un tercer respaldo efectuado semestralmente, el cuál deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.
* Cualquier situación anómala y contraria a la seguridad deber se documentada, posterior revisión de los registros o Log de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, ya sea que se encuentre en el ámbito legal o administrativa.

## Nivel 2: Seguridad Lógica

### Control de Acceso

* El Director del proceso de TIC’s debe proporcionar toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, instructivos, documentos, matrices, otros, localizados en el sistema de gestión de la calidad.

#### Administración del acceso a los usuarios

* Son usuarios de la red empresarial los empleados contratados directamente bajo cualquier modalidad de contrato, que tenga contacto directo y utilice cualquier recurso tecnológico de Galotrans.
* Cada líder de proceso solicitará las cuentas de acceso a las aplicaciones requeridas, detallando los permisos y funciones que estarán a cargo del funcionario, además de sus datos personales y objetivo de su uso. Esta solicitud deberá estar aprobada por la dirección de TICs, a través de la respuesta a los requerimientos realizados por el responsable del proceso. Las autorizaciones sobre los permisos de usuarios en Ofimatica serán autorizados por la gerencia general.
* No se proporcionará el servicio solicitado por un usuario, o proceso, sin antes haber completado todos los procedimientos de autorización necesarios para su ejecución según el sistema de gestión de calidad.
* La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres, teniendo en cuenta los siguientes los requerimientos:
  + Al menos una letra en mayúscula.
  + Al menos una letra en minúscula.
  + Al menos dos números.
  + Al menos un carácter especial.
* Se requiere el cambio de la (las) contraseña(s) por parte del usuario cada 3 meses, de todas la cuentas de acceso sobre los sistemas a los cuales tiene acceso.

#### Responsabilidades del usuario

##### Generales

* El usuario es responsable exclusivo de mantener a salvo su contraseña.
* El usuario será el único responsable del uso que haga con su cuenta de acceso a los sistemas o servicios.
* Se debe evitar el guardar o escribir las contraseñas en lugares donde pueden encontrarse expuestas.
* El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él cuando se ausente del mismo. El usuario deberá bloquear el acceso al sistema operativo por medio de la combinación de teclas Ctrl + Alt +Supr y seleccionando la opción “bloquear equipo”.
* Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas tecnológicos de la empresa está obligado a reportarlos a los administradores de tecnología.

##### Uso correo electrónico

* El correo electrónico es de uso exclusivo de los empleados y con fines netamente laborales.
* Todo uso indebido del servicio de correo electrónico será penalizado de acuerdo a la gravedad del acto y dicha penalización estará a disposición de la alta dirección.
* El usuario será responsable de la información que sea enviada con su cuenta.
* Los administradores de la red empresarial, podrán monitorear las cuentas de los usuarios que presenten un comportamiento sospechoso para la seguridad de la red, con la respectiva autorización de la alta dirección.
* El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento de autor.

#### Control de acceso a la red

* El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, haciendo uso de un mecanismo de autenticación.
* Se registrará todo el acceso a los dispositivos de red, mediante los archivos de log, de los dispositivos que provean esta facultad.

#### Control de acceso al sistema operativo

* Se crearán dos cuentas en el sistema operativo de cada uno de los equipos de la empresa, una cuenta con privilegios administrativos para el acceso a los administradores de tecnología, y otra cuenta con privilegios limitados para el usuario final.
* Cada vez que el usuario abandone temporalmente su puesto de trabajo, éste debe bloquear su equipo de trabajo, para proteger el acceso por parte de terceros a la información allí contenida.

##### Servidores

* El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido a los administradores de tecnología.

#### Control de acceso a las aplicaciones

* Las aplicaciones deben estar correctamente diseñadas, por medio de un sistema de gestión de permisos, los cuales permitirán controlar los accesos y facultades a los módulos del aplicativo.
* Debe realizarse seguimiento a la edición de las solicitudes de servicio de los clientes, a través de un sistema de registro sobre las modificaciones realizadas, con el fin de determinar el usuario, fecha, hora y valor cambiado.

### Gestión de Operaciones

#### Protección contra software malicioso

* Se adquirirá y utilizará software únicamente de fuentes confiables. El proceso de tecnología aprobará y publicará el software permitido en el documento matriz de aplicaciones (GLT-GT-M-01). No se podrá instalar ningún software que no se encuentre en dicho documento, sin la previa validación y autorización del director de TICs.
* Las estaciones de trabajo y los servidores tendrán instalado, activado y configurado correctamente el software de Antivirus, teniendo en cuenta los módulos de protección en tiempo real y firewall.
* Por ningún motivo está permitido ejecutar programas sospechosos enviados al correo.
* Es responsabilidad de cada usuario reportar al proceso de TICs, cualquier incidencia con respecto a la seguridad de los recursos de tecnología que éste maneje.

#### Mantenimiento

* El mantenimiento de los aplicativos y sistemas de software son de exclusiva responsabilidad del proceso de TICs.
* El cambio de los archivos del sistema operativo de los equipos, no está permitido.
* El analista de sistemas llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

#### Copias de seguridad

* Los respaldos sobre las bases de datos de los sistemas de información críticos de la empresa se realizarán a diario.
* Las copias no se almacenarán en los servidores compartidos, sino en el equipo del director de tecnología, en el cual, cada semana se realizará una sincronización con el servicio de google drive en la nube de la última copia realizada sobre cada uno de los respaldos de las bases de datos.

#### Manejo y seguridad de medios de almacenamiento

* Los medios de almacenamiento con información sensible o copias de respaldo deberán ser manipuladas única y exclusivamente por el analista de sistemas, asegurando la información contenida en los mismos.
* Todo medio de almacenamiento con información sensible, será guardado bajo llave y ésta será guardada por el analista de sistemas.

## Nivel de Seguridad Física

### Resguardo de los equipos de tecnología

* La intervención física de los usuarios o terceros está totalmente prohibida sobre los recursos tecnológicos, salvo autorización o supervisión de los administradores de sistemas.
* El soporte técnico a los equipos de trabajo, servidores y redes, es responsabilidad del proceso de TICs.
* Los cuartos de comunicaciones, son zonas restringidas, únicamente accesibles por personal autorizado. Estas zonas están protegidas bajo llave, la cual debe estar a cargo de los Administradores de TICs.

### Controles físicos generales

* Cada seis meses se programa un mantenimiento preventivo sobre el hardware de cada uno de los equipos de cómputo de la empresa, teniendo en cuenta, routers, estaciones de trabajo, servidores, acces point, switchs, etc. El registro del mantenimiento se llevará a cabo con el formato (GLT-GT-F-01).
* Al finalizar la jornada laboral cada usuario debe verificar el correcto apagado del equipo, esto con el fin de prolongar la vida útil del mismo.

### Actividades Prohibidas

* Está rotundamente prohibido el ingreso de bebidas o alimentos de cualquier tipo a los centros de datos.

## Seguridad Legal

### Cumplimiento de requisitos legales

* Las acciones de los empleados de Galotrans S.A, al respecto de la utilización de software pirata dentro de las instalaciones de la empresa, no son propias de Galotrans.
* La empresa se reserva todo derecho al utilizar software licenciado en los equipos que considere necesarios. Además de ello, se promueve la utilización de software libre, teniendo en cuenta el tipo de licencia y el apoyo a la respectiva comunidad.
* Bajo ninguna circunstancia Galotrans S.A aprueba o autoriza la utilización de software sin licencia en cualquiera de los equipos de cómputo, en sus instalaciones.
* El director de tecnología se encargará de archivar cada una de las licencias (privativas o libres) y contratos, de los sistemas de software adquiridos por la empresa para su infraestructura tecnológica.
* La empresa no participa con sus empleados en la adquisición de software no legal.
* La empresa no da el aval a sus empleados para que puedan instalar software no licenciado en los equipos de trabajo, los cuales son propiedad exclusiva de Galotrans S.A.
* Galotrans S.A respeta los contratos de licencia de usuario final del software comercial con derechos de copyright, como de software libre con derechos de copyleft.