Cataluña Transporte de Carga
Logística especializada

SISTEMA DE GESTIÓN INTEGRAL

MANUAL DE TECNOLOGIA E INFORMATICA

Código: G-004-M **Revisión: 7** **Fecha: 31 de JULIO de 2017**

REVISADO POR: Gerente Administrativo y Financiero **Firma:** _____

APROBADO POR: Gerente General **Firma:** _____

HOJA DE CONTROL DE CAMBIOS

REV	NATURALEZA DEL CAMBIO	FECHA	APROBO
4	Ajustes del manual según requerimientos de la Norma ISO 28000	04-03-2014	GG
5	Se dejó como responsable al Gerente administrativo y se quitó la figura del oficial de cumplimiento ya que es la misma persona; Se complementó el ítem 4.5.2 con la leyenda del correo electrónico; Se incluyeron los formatos establecidos en las etapas correspondientes	29-05-2015	GG
6	Ajuste de Copias de Seguridad al Google Drive, numeral 4.7.	26-05-2016	GG
7	Incorporación de las sanciones por el incumplimiento del manual de tecnología e informática	31-07-2017	GG

REGISTROS ASOCIADOS

Control de equipos, licencias y contraseñas
Control backup

LISTA DE DISTRIBUCIÓN

COPIA	DISTRIBUCIÓN
COPIA MAGNETICA	REPRESENTANTE DEL SISTEMA
Firma:	

TABLA DE CONTENIDO

1. DISPOSICIONES GENERAL 3

1.1 AMBITO DE APLICACIÓN Y FINES 3
1.2 BENEFICIOS 3

2. POLITICA GENERAL DE TECNOLOGIA E INFORMATICA 3

2.1 OBLIGACIONES DE LOS USUARIOS 3

3. POLITICAS Y ESTANDARES DE SEGURIDAD FISICA Y AMBIENTAL 4

3.1 RESGUARDO Y PROTECCION DE LA INFORMACION 4
3.2 CONTROLES DE ACCESO FISICO 4
3.3 PROTECCION Y UBICACIÓN DE LOS EQUIPOS 4
3.4 MANTENIMIENTO DE EQUIPO 5
3.5 PERDIDA DE EQUIPO 5
3.6 DAÑO DEL EQUIPO 6

4. POLITICAS Y ESTANDARES DE SEGURIDAD Y ADMINISTRACION DE OPERACIONES DE CÓMPUTO 6

4.1 INSTALACION DE SOFTWARE 6
4.2 USO DE MEDIOS DE ALMACENAMIENTO 6
4.3 IDENTIFICACION DEL INCIDENTE 6
4.4 SEGURIDAD PARA LA RED 7
4.5 USO DEL CORREO ELECTRONICO 7
4.6 CONTROLES CONTRA CODIGO MALICIOSO 7
4.7 COPIAS DE SEGURIDAD 8
4.8 INTERNET 8

5. POLITICAS Y ESTANDARES DE CONTROLES DE ACCESO LOGICO 8

5.1 CONTROLES DE ACCESO LOGICO 8
5.2 ADMINISTRACION DE PRIVILEGIOS 9
5.3 EQUIPO DESATENDIDO 9
5.4 ADMINISTRACION Y USO DE CONTRASEÑA 10

6. SANCIONES 10

ANEXO I : INFORMACION SENSIBLE POR PROCESO

INTRODUCCION

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de las políticas y estándares.

La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de CATALUÑA S.A. en materia de seguridad.
Este documento se encuentra estructurado en cuatro políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

• Seguridad de Personal.

• Seguridad Física y Ambiental.

• Administración de Operaciones de Cómputo.

• Controles de Acceso Lógico.

1. DISPOSICIONES GENERALES

1.1 Ámbito de Aplicación y Fines

Las políticas y estándares de Seguridad Informática tienen por objeto establecer medidas técnicas y de organización de las tecnologías de información y de las personas que interactúan haciendo uso de los servicios informáticos que proporciona CATALUÑA S.A. y contribuyendo con la función informática a la mejora y complimiento de metas institucionales.

1.2 Beneficios

Las políticas y estándares de seguridad informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de la organización

2. POLITICA GENERAL DE TECNOLOGIA E INFORMATICA

CATALUÑA TRANSPORTE DE CARGA S.A. Se encuentra comprometida con la excelente administración y control a nivel tecnológico e informático, destina herramientas para la protección y aseguramiento de su información sensible y el correcto funcionamiento del hardware y software de la compañía, implementando nuevos programas y actualizaciones, evitando al máximo los riesgos informáticos y reducir los daños graves tanto en hardware como en software ó por pérdida o fuga de información.
Es de carácter obligatorio por parte de los usuarios de CATALUÑA S.A. el uso adecuado, seguro y responsable de los equipos que le sean asignados, en cumplimiento de los lineamientos establecidos por parte de la compañía.

2.1 Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

3. POLITICAS DE SEGURIDAD FISICA Y AMBIENTAL

3.1 Resguardo y Protección de la Información

3.1.1 El usuario deberá reportar de forma inmediata al gerente administrativo cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

3.1.2 El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.

3.2 Controles de Acceso Físico de Equipos de Cómputos

3.2.1 Cualquier persona que tenga acceso a las instalaciones de la Compañía, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de CATALUÑA S.A., en el área de recepción.

3.2.2 Los computadores portátiles y cualquier activo de tecnología de información, podrá salir de la compañía únicamente con la autorización y el visto bueno de la Gerencia General y/o la Dirección Administrativa.

3.2.3. Control de acceso instalaciones a través de Tarjetas de Proximidad en todas las áreas excepto sala de juntas para todos los miembros de la organización.

3.3 Protección y Ubicación de los Equipos

3.3.1 Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Gerente administrativo, en caso de requerir este servicio deberá solicitarlo.

3.3.2 La Gerencia Administrativa y Financiera será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada.

3.3.3 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones encomendadas al funcionario de CATALUÑA S.A.

3.3.4 Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

3.3.5 Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro identificada como “Mis Documentos” ya que las otras están destinadas para archivos de programa y sistema operativo.

3.3.6 Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos

3.3.7 Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

3.3.8 Se debe mantener el equipo informático en un entorno limpio y sin humedad.

3.3.9 El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables a través de solicitud de mantenimiento al correo m_vargas@catalunatransporte.com

3.3.10 Queda prohibido que el usuario abra o desarme los equipos de cómputo.

3.4 Mantenimiento de Equipo

3.4.1 Únicamente el personal autorizado por el Gerente administrativo y el Técnico Autorizado de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático, dejando los respectivos soportes de la actividad realizada a cada equipo según el caso.

3.4.2 Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

3.5 Pérdida de Equipo

3.5.1 El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo, lo cual corresponde a asumir el costo del equipo.

3.5.3 El usuario deberá dar aviso inmediato al Gerente Administrativo de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo, quien procederá a hacer el bloqueo correspondiente de claves y accesos.

3.6 Daño del Equipo
El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.

4. POLITICAS DE ADMINISTRACION DE OPERACIONES DE CÓMPUTO

4.1 Instalación de Software
4.1.1 Los usuarios que requieran la instalación de software que no sea propiedad de la Compañía, deberán justificar su uso y solicitar su autorización por escrito al Gerente administrativo indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá la mencionada instalación. Dicha instalación sólo puede ser realizada por el Gerente Administrativo mediante una Clave Secreta que sólo él Administra la cual está en el formato “control equipos, licencias y contraseñas”

4.1.2 Se considera una falta grave el que los usuarios falsifiquen la clave Administradora e instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado de la compañía, que no esté previamente autorizado.

4.2 Uso de Medios de Almacenamiento

4.2.1 El Técnico Autorizado de Sistemas y el Gerente Administrativo deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

4.2.2 Las actividades que realicen los usuarios de Informática son registradas y susceptibles de auditoría

4.3 Identificación del Incidente

4.3.1 El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Gerente Administrativo lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

4.3.2 Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificarse.

4.3.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de CATALUÑA S.A. debe ser reportado.

4.4. Seguridad para la Red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Gerente Administrativo y el Técnico Autorizado de Sistemas, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de CATALUÑA S.A., así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

4.5 Uso del Correo Electrónico

4.5.1 Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa de CATALUÑA S.A., a menos que cuente con autorización.

4.5.2 Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de CATALUÑA S.A. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor. Todas firmas del correo cuentan con los logos de la empresa y las certificaciones vigentes, así como la leyenda para dar cumplimiento con la Ley 1581 2012 (protección datos personales) así:

"Este mensaje y sus anexos está dirigido para ser usado por su(s) destinatario(s) exclusivamente y puede contener información confidencial y/o reservada protegida legalmente. Si usted no es el destinatario, se le notifica que cualquier distribución o reproducción del mismo, o de cualquiera de sus anexos, está estrictamente prohibida. Si usted ha recibido este mensaje por error, por favor notifíquenos inmediatamente y elimine su texto original, incluidos los anexos, o destruya cualquier reproducción del mismo. Las opiniones expresadas en este mensaje son responsabilidad exclusiva de quien las emite y no necesariamente reflejan la posición institucional de CATALUÑA TRANSPORTE DE CARGA S.A., ni comprometen la responsabilidad institucional por el uso que el destinatario haga de las mismas. Este mensaje ha sido verificado con software antivirus. En consecuencia, CATALUÑA TRANSPORTE DE CARGA S.A. no se hace responsable por la presencia en él, o en sus anexos, de algún virus que pueda generar daños en los equipos o

programas del destinatario. Antes de imprimir este mensaje, asegúrese que es necesario. Proteger el medio ambiente está también en sus manos!"

4.5.3 Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

4.5.4 Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

4.6 Controles contra código malicioso

4.6.1 Para prevenir infecciones por virus informático, se ha instalado un Firewall que bloquea el ingreso a páginas no autorizadas por la Compañía por tener contenidos que pueden poner en riesgo los equipos de cómputo. Los usuarios de CATALUÑA S.A. no deben hacer uso de software que no haya sido proporcionado y validado por los autorizados.

4.6.2 Los usuarios de CATALUÑA S.A. deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado.

4.6.3 Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

4.6.4 Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización.

4.6.5 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y comunicar al Gerente administrativo para la detección y erradicación del virus.

4.6.6 Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la CATALUÑA S.A. en: Antivirus, Outlook, office, Navegadores u otros programas.

4.6.7 Debido a que algunos virus son extremadamente complejos, ningún usuario de CATALUÑA S.A. debe intentar erradicarlos de las computadoras.

4.7 Copias de Seguridad

Toda la información se encuentra almacenada en servidores de uso externo que garantizan la seguridad y el uso de la información mediante Internet en cualquier equipo autorizado que cuente con las claves de acceso correspondientes. Los registros de la copias de seguridad quedan en el formato "control backups" únicamente para los registros de información sensible del proceso de seguridad. La información sensible está disponible en el anexo 1.

Como un control adicional, cada funcionario de la Compañía cuenta con el acceso a la nube de Google Drive desde su correo corporativo. Es responsabilidad de cada uno almacenar la información que se encuentra en el servidor estableciendo los controles de privacidad para la

información sensible. En caso de contar con información sensible ajena al Google Drive, se llevara a cabo la copia de seguridad empleando el formato correspondiente.

4.8 Internet

4.8.1 El acceso a Internet provisto a los usuarios de CATALUÑA S.A. es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña, para lo cual solicitarán clave de acceso.

4.8.2 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por CATALUÑA S.A. en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada previamente.

4.8.3 Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización
- La utilización de Internet es para el desempeño de su función y puesto en la organización y no para propósitos personales.

5. POLITICAS Y ESTANDARES DE CONTROLES DE ACCESO LOGICO

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de CATALUÑA S.A., por lo cual deberá mantenerlo de forma confidencial.

5.1Controles de Acceso Lógico

5.1.1 Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

5.1.2 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos antes de poder usar la infraestructura tecnológica de CATALUÑA S.A.

5.1.3 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de CATALUÑA S.A., a menos que se tenga el visto bueno del dueño de la información y de la autorización expresa de la Gerencia General.

5.1.4 Cada usuario que acceda a la infraestructura tecnológica de CATALUÑA S.A. debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.

5.1.5 Los usuarios son responsables de todas las actividades

5.2 Administración de Privilegios
Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al Gerente Administrativo para el cambio de privilegios.

5.3 Equipo Desatendido
Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados cuando no se encuentren en su lugar de trabajo.

5.4 Administración de Contraseña
5.4.1 La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

5.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Gerente Administrativo para que se le proporcione una nueva contraseña.

5.4.3 Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

5.4.4 Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con la misma.

5.4.5 Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.

5.4.6 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

5.5.7 Registro de claves y licencias tiene toda la información de los equipos en Cataluña y claves asignadas al personal por parte del gerente administrativo, de igual manera se mantiene actualizado un inventario de equipos en el formato establecido “control equipos, licencias y contraseñas”

5.5.8. Las contraseñas de acceso a los equipos serán actualizadas anualmente o según los riesgos identificados según proceso o por gerencia.

5.5.9.. Se estipulan controles en las inspecciones de seguridad para verificar que los equipos tienen claves de acceso, bloqueos automáticos, antivirus y demás aspectos que permitan evidenciar cumplimiento de la política informática.

6. SANCIONES

El incumplimiento de alguno de los enunciados anteriores está directamente relacionado con lo descrito en el reglamento interno de trabajo, especialmente en los capítulos relacionados con: XX “Escala de faltas y sanciones”; XXII “Procedimiento para comprobación de faltas y normas de aplicación de sanciones disciplinarias”. Adelantado el debido proceso y teniendo en cuenta el impacto de la falta, se determinará la sanción a aplicar: Llamado de atención, amonestación, multa, suspensión del cargo o terminación unilateral con justa causa.

ANEXO 1 – INFORMACION SENSIBLE POR PROCESO

PROCESO	INFORMACION SENSIBLE
SEGURIDAD (*)	Hojas de vida trafico (Estudios de seguridad, soportes, acuerdos)
ADMINISTRATIVO – CONTABILIDAD	Bases datos (proveedores y terceros), Nómina, Reportes UIAF, Pagos, Legalizaciones, Estudios a clientes, Reportes, facturación, seguros
ADMINISTRATIVO – GESTION HUMANA	Hojas de vida, Seguridad social mensuales, sistema de gestión
OPERACIONES Y FLOTA PROPIA	Operaciones: Trazabilidad de la operación, Reportes de enturnamiento, Soportes fotográficos impo y expo (DTA y OTM), Inventarios y asignación de precintos) Flota propia: Ejecución mantenimiento-programa; hoja de vida vehículos, hoja de vida personal, documentos vencibles; kilometraje/peajes/gastos/liquidaciones.
COMERCIAL	Cotizaciones, Presentaciones, Costos, Ofertas comerciales, Bases de datos
GESTION INTEGRAL	Carpeta SGI (Documentos y registros)
GERENCIA	Syscar

(*) Backup disco duro externo.