DIRECTIVA GERENCIAL No. TDD1020

NORMAS DE SEGURIDAD Y CONTROL DE LA TECNOLOGÍA INFORMÁTICA DE TRANSELCA S.A. E.S.P.

1. OBJETIVO

Mediante el presente documento se definen la política fundamental, las responsabilidades y las normas a tener en cuenta en TRANSELCA, para garantizar la seguridad y control de la infraestructura de Tecnología Informática - TI y de la información administrada a través de ella.

2. POLÍTICA

Es política de TRANSELCA proporcionar a sus empleados la tecnología informática necesaria para efectuar sus actividades laborales y para su crecimiento profesional y personal, teniendo en cuenta el cumplimiento de las Normas que regulan el buen uso de los recursos. Se debe mantener altos estándares de seguridad y control de los procesos efectuados a través de la misma, con el fin de proteger la información, hardware, software y redes contra daños accidentales o intencionales y asegurar la integridad, disponibilidad y oportunidad de estos recursos.

Esta Directiva Gerencial se encuentra enmarcada dentro de los elementos de Filosofía Corporativa de la empresa como lo son la Seguridad, el Comportamiento Ético, y Servicio Profesional.

	Fecha de Vigencia:	Fecha Próxima Revisión:	Actualización Nº:	Copia Nº:
Gerente General	7 de Diciembre de 2017	Febrero de 2018	16	

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

3. CONTENIDO

CAPITULO 1. ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA
1.1. COMITÉ DE SEGURIDAD INFORMÁTICA

El Comité de Seguridad Informática es un órgano interdisciplinario conformado por:

- Gerente Administrativo.
- Jefe del Departamento Gestión de la Información.
- Coordinador de la Seguridad informática.
- Un representante de Auditoría Interna
- Un representante de Secretaría General
- Adicionalmente cuando se requiera, se invitará al comité, a representantes de otras Gerencias y/o Direcciones de TRANSELCA.

Es de carácter obligatorio la asistencia del personal antes nombrado, o en su defecto, de un representante.

Este comité se reunirá cada vez que se requiera, y en estas reuniones, de acuerdo con las políticas establecidas, se tomarán las decisiones para la implementación y actualización del esquema de seguridad en los diferentes sistemas de información de la empresa. El Coordinador de la Seguridad Informática será el custodio de las actas del comité.

El Comité de Seguridad delegará en el Departamento de Talento Humano la comunicación de las sanciones a aplicar a los usuarios que incumplan la presente Directiva, dichas comunicaciones se harán por medio de un memorando enviado al usuario que incumplió lo establecido en la Directiva TDD1020.

Responsabilidades

- Formular las políticas, metas y objetivos de la seguridad de TI y coordinar su aprobación por parte de la Gerencia General.

- Brindar apoyo a las acciones y medidas definidas para el mejoramiento, difusión y cumplimiento de las políticas de seguridad.

- Aprobar programas y planes relacionados con la seguridad de la Tecnología Informática.
- Apoyar al crecimiento y expansión de los proyectos en seguridad informática.
- Definir y aprobar las sanciones respectivas en caso del incumplimiento de las políticas de seguridad establecidas.
- Definir políticas generales para el cumplimiento de la normatividad legal sobre el uso del software en TRANSELCA.

1.2. RESPONSABILIDADES DE LOS DEPARTAMENTOS CUSTODIOS DE LOS SISTEMAS DE INFORMACIÓN DE TRANSELCA

- Investigar y recomendar esquemas de seguridad, aplicando las mejores tecnologías, de acuerdo a evaluaciones costo-beneficio.
- Divulgar políticas y recomendaciones de seguridad para prevenir incidentes de seguridad en los sistemas informáticos.
- Velar por el cumplimiento de las políticas de seguridad informática.
- Velar por el cumplimiento de la normatividad legal sobre el uso del software en la empresa.
- Promover en los trabajadores el empoderamiento de la administración de la información, con el fin de reforzar el autocontrol y el cumplimiento de las políticas de seguridad establecidas.
- Promover el compromiso y la participación de todos los trabajadores en la conformación del ambiente de seguridad de la organización.
- Administrar la seguridad de los sistemas de bajo su administración.
- Organizar, implementar, supervisar y monitorear los esquemas de seguridad definidos sobre los sistemas de Informática, de acuerdo con las políticas de seguridad aprobadas por el comité.
- Aplicar los procedimientos e instructivos definidos de acuerdo a las políticas de seguridad.
- Evaluar e informar al comité acerca de la eficacia de los esquemas de seguridad implantados.
- Operar, dar soporte y/o monitorear el hardware y las redes y desarrollar, administrar y dar mantenimiento al software utilizado.

1.3. RESPONSABILIDADES DE LOS USUARIOS

- Es responsabilidad de los Usuarios de la infraestructura de tecnología informática, cumplir con las normas enunciadas en la presente Directiva.
- Informar oportunamente y de acuerdo lo definido en el Instructivo TIA5001 al Coordinador de Seguridad Informática, cuando conozcan o intuyan de incumplimiento de las políticas por parte de otro (s) usuarios.

CAPÍTULO 2. CLASIFICACIÓN Y CONTROL DE LA INFORMACIÓN

Las siguientes normas deben ser aplicadas en las actividades relacionadas con el manejo de la información administrada a través de las herramientas de tecnología informática, con el fin de protegerla, ya sea ésta de propiedad de la empresa o de terceros. Estas normas son de obligatorio cumplimiento por parte de los Trabajadores y Contratistas de la empresa.

2.1. RESPONSABILIDADES DEL DUEÑO DE LA INFORMACIÓN

- Establecer el valor de la información y su criticidad.
- Revisar los resultados de la evaluación de riesgos y definir según estos el diseño, el alcance y el costo de las medidas de seguridad y los controles a establecer, con el fin de proteger la información contra daños accidentales o intencionales.
- Definir controles alternos que mitiguen el riesgo, en aquellos casos en que las medidas de control sugeridas en la práctica no resulten viables o demasiado costosas.
- Autorizar el acceso a la información a los usuarios, especificando las características y niveles de acceso.
- Velar por el cumplimiento de los controles establecidos para la protección de la información bajo su responsabilidad.
- Verificar la existencia de un plan de recuperación de los servicios, documentado y comprobado periódicamente para los procesos críticos del negocio.

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

2.2. RESPONSABILIDADES DEL CUSTODIO DE LA INFORMACIÓN

- Implementar los controles establecidos por el Dueño de la Información.
- Documentar la evaluación de riesgos y exposiciones potenciales de la información y establecer requerimientos de control.
- Administrar los accesos a la información bajo su responsabilidad, de manera que las personas autorizadas por el Dueño de la Información sean las únicas que tengan acceso a ella.

Para definir el nivel de protección requerido, los dueños deben clasificar la información según las siguientes categorías:

2.2.1 Por tipo de propiedad

Confidencial

Concepto establecido en la Política de información y del conocimiento: hacia la valoración estratégica de los activos del conocimiento del Grupo Empresaria ISA.

Privada

Es aquella información que pertenece a un particular y que hace parte de su intimidad.

Pública

Concepto establecido en la Política de información y del conocimiento: hacia la valoración estratégica de los activos del conocimiento del Grupo Empresaria ISA.

2.2.2. Por Criticidad de la información

Vital

Es aquella que es esencial para la continuidad de las actividades de la empresa. Esta información es irremplazable porque provee evidencia del status legal, de la propiedad y de las finanzas.

Importante

Es aquella que es necesaria para la continuidad de las actividades de la empresa. Aunque esta información puede ser reemplazada o recuperada, el costo de hacerlo es muy alto en tiempo y en dinero.

Útil

Cuando se requiere para la operación ininterrumpida de la empresa. Esta información es reemplazable o se puede recuperar rápidamente causando problemas temporales a la empresa.

No esencial

Es aquella que no agrega valor a las operaciones de la empresa y en consecuencia puede ser destruida.

CAPITULO 3. SEGURIDAD CON EL PERSONAL

Con el fin de reducir los riesgos por error humano, robo, fraude o mal uso de facilidades, se han definido las siguientes normas:

- El Departamento de Talento Humano debe verificar que en la Descripción de Responsabilidades Asignadas (DRA), cada trabajador defina sus responsabilidades con los Sistemas de Información y los equipos de Tecnología Informática inherente al cargo que desempeña.
- Todos los Trabajadores y Contratistas de la empresa deben firmar un acuerdo de compromiso de buen manejo de las herramientas de Tecnología Informática que se les asigne.
- El Departamento Gestión de la Información realizará periódicamente actividades para divulgar las normas contenidas en esta directiva y las recomendaciones de seguridad informática, cuando se considere necesario.
- Cuando ocurran incidentes de seguridad relacionados con los sistemas de tecnología informática, los trabajadores y/o Contratistas involucrados deben realizar, tan pronto como sea posible, el reporte correspondiente y entregarlo al Coordinador de Seguridad Informática.

- Los trabajadores y/o Contratistas deberán notificar inmediatamente al Coordinador de Seguridad Informática, acerca de cualquier sospecha referente a debilidades de seguridad (o amenazas) al sistema o a los servicios.
- TRANSELCA podrá adelantar un proceso disciplinario contra los trabajadores y/o terceros que hayan incumplido las políticas y procedimientos de seguridad.

CAPÍTULO 4. SEGURIDAD FÍSICA

Con el fin de prevenir el acceso no autorizado, daño o interferencia en los servicios de TI se han definido las siguientes normas cuyo cumplimiento será vigilado por los Departamentos Custodios de los Sistemas de Información:

- Las instalaciones donde se encuentran los diferentes servidores y otros equipos de TI críticos, deben garantizar las condiciones técnicas exigidas para la seguridad y correcto funcionamiento de ellos, tales como suministro de potencia ininterrumpida UPS, control de acceso y de temperatura, sistema contra incendios, piso falso, entre otros.
- El acceso a las salas de servidores y a los equipos críticos sólo debe permitirse al Administrador del mismo y al personal debidamente autorizado (personal de mantenimiento y visitante).
- Todos los visitantes a las instalaciones donde se encuentran los servidores y los equipos críticos deben ser acompañados por el administrador.
- El ingreso y salida de elementos a las instalaciones donde se encuentran los servidores debe estar controlado por los administradores de los diferentes sistemas.
- Todos los equipos de comunicación y de cómputo deben estar conectados a un sistema de corriente regulada. Los servidores y las estaciones de trabajos críticas deben estar conectados a un sistema de corriente regulada ininterrumpida.
- Las instalaciones donde se encuentran los servidores no deben utilizarse como bodega de almacenamiento de insumos (papelería, cintas y equipos fuera de uso). Se debe reducir al mínimo el nivel de material combustible.
- La consola o terminal principal del servidor no debe utilizarse para la operación de las aplicaciones

- Se debe realizar mantenimiento preventivo y correctivo a todos los recursos físicos y de los mecanismos de protección del ambiente computacional.
- Los manuales del software y el hardware y los procedimientos escritos que soportan las labores de recuperación en casos de contingencia, la operación de los sistemas y los cambios de programas, deben reposar en un sitio conocido y a cargo del custodio del Sistema de Información respectivo. Los manuales de usuario final deben estar disponibles en la intranet para el acceso por parte de ellos.
- Debe existir un inventario actualizado de hardware y software que componen cada uno de los sistemas de la empresa y debe ser administrado por el Custodio del Sistema.
- El cableado eléctrico y de datos debe estar identificado en forma clara.
- Cuando se requiera trasladar equipos o software fuera de las instalaciones de la empresa, se deben cumplir los procedimientos definidos para estos casos.

CAPÍTULO 5. ADMINISTRACIÓN Y USO DE REDES, SERVIDORES Y ESTACIONES DE TRABAJO

5.1. RESPONSABILIDADES

Con el fin de asegurar la correcta y segura operación de la administración de redes y de los servidores, se han definido las siguientes responsabilidades para el Administrador de la Red y para los Administradores de los Servidores:

- Mantener los instructivos y procedimientos para la administración y operación de los sistemas de red y de servidores.
- Mantener altos niveles de seguridad en los sistemas de red y de servidores utilizados, aplicando las mejoras y arreglos de seguridad requeridos para esto.
- Revisar la capacidad de los sistemas de red y de servidores y proyectar la capacidad y tecnología requerida en un futuro, dependiendo del crecimiento de los servicios actuales y de implantaciones de servicios adicionales.
- Asegurar que los procedimientos de recuperación y respaldo apropiados se establezcan para cada servicio, determinando su frecuencia, de acuerdo a la criticidad establecida por el Dueño de la información.

- Aplicar en los equipos de comunicación y servidores los esquemas de seguridad definidos para controlar el acceso a ellos y a sus utilidades.
- Establecer los procesos de monitoreo para el uso de los sistemas de red y de servidores y mantener los rastros de auditoría sobre eventos de seguridad.
- Reportar a la Mesa de Ayuda (Línea 73000) las fallas concernientes a los sistemas de red y de servidores.
- Tomar medidas especiales para prevenir y/o detectar ataques a los sistemas de red y de servidores a su cargo.
- Proteger la documentación del sistema contra el acceso no autorizado.
- El Administrador de la Red debe manejar la seguridad en las redes con especial cuidado, encriptando y protegiendo la información sensible que viaja a través de redes de dominio público y según un estudio costo beneficio del riesgo asociado.
- Los Administradores de los Servidores debe mantener actualizado el antivirus para los servidores a su cargo.
- El Administrador de los Servidores debe monitorear el ambiente donde estos se encuentran.

5.2. POLÍTICA DE RESPALDO Y RECUPERACIÓN DE INFORMACION

El Administrador del Servidor debe velar por:

- El almacenamiento en un lugar seguro, de los medios magnéticos que contienen el respaldo de la información del servidor. Este lugar debe poseer control de acceso y de temperatura y sistema contra incendios.
- Definir la rotación con que se manejarán los medios magnéticos que contienen el respaldo, en todo caso Se deberá cumplir con las políticas generales que se definan en el comité de seguridad al respecto.
- La programación de pruebas aleatorias a los medios de respaldo, de manera tal que se pruebe la recuperación de información de todos los servicios de TI a cargo del Departamento Gestión de la Información. Para las pruebas se deberá utilizar la cinta de fin de mes más reciente.
- Los medios magnéticos que contienen las copias de respaldo del tercer y quinto día hábil de la semana, deben ser enviados para su custodia en un sitio alterno con medidas de control de temperatura, de acceso y protegidos por un sistema

contraincendios. Estos medios retornarán a la sede de la empresa en el servicio del mismo día de la semana siguiente.

- El transporte debe ser realizado por personal que conozca la importancia del objeto que transportan.
- Conocer en todo momento, la ubicación de los medios de respaldo del equipo a su cargo.

5.3. INTERCAMBIO DE DATOS

La Gerencia Dueña de la Información debe firmar acuerdos formales cuando desee establecer transferencias electrónicas entre la empresa y otras organizaciones, para lo cual se deben cumplir con los estándares establecidos para proteger la información en tránsito, asegurando que la información viaje encriptada cuando la comunicación se haga a través de redes de acceso público.

5.4. PROTECCIONES CONTRA LOS VIRUS

- El Departamento Gestión de la Información velará por la disponibilidad del software antivirus actualizado para que sea aplicado en los servidores por sus administradores.
- El Departamento Gestión de la Información velará porque todas las estaciones de trabajo, posean instaladas herramientas actualizadas para la detección y prevención de virus.
- En caso de que en una estación de trabajo no se pueda ejecutar el antivirus, es responsabilidad del Usuario informar oportunamente al Departamento Gestión de la Información. Cuando el Usuario sospeche que un virus ha intentado o se ha instalado en su estación de trabajo, debe notificarlo inmediatamente al Departamento Gestión de la Información, quien deberá verificar esta situación y realizará los correctivos correspondientes.
- Cuando el Departamento Gestión de la Información verifique la existencia de un virus que por su naturaleza represente una amenaza a la red y estaciones de TRANSELCA, deberá informar en forma clara y oportuna a todos los Usuarios de la red acerca del virus detectado y sobre el procedimiento a seguir para minimizar el riesgo asociado.

- Es responsabilidad de los Usuarios seguir las recomendaciones del Departamento Gestión de la Información en lo concerniente al manejo de los virus.

5.5. NORMAS PARA LA ADMINISTRACIÓN DE REDES

- El Administrador de la Red debe asegurar el establecimiento de controles apropiados para garantizar la seguridad de la información en redes, al igual que protección a servicios conectados contra accesos no autorizados.
- El Administrador de la Red creará el acceso a la red a los nuevos Usuarios.
- Cuando un trabajador nuevo en la empresa, necesita para el desarrollo de sus actividades acceso a la red y/o a cualquier Sistema de Información, el encargado en el Departamento al cual pertenecerá el trabajador deberá realizar la respectiva solicitud de acuerdo al instructivo para Administración y registro de accesos a los sistemas de información TIA5004.
- En el caso de un trabajador que ya se encuentre laborando en la empresa, el acceso a la red antes mencionada, debe ser solicitado por el jefe del Departamento al cual pertenece el funcionario, de acuerdo al instructivo para Administración y registro de accesos a los sistemas de información.
- Es responsabilidad del Administrador de cada red definir las configuraciones de red de todos los equipos conectados a ella.
- Por ningún motivo los Usuarios podrán modificar su configuración de la red. Sin embargo, en casos especiales, cuando sea requerido hacer modificaciones en la configuración de red en alguna estación de trabajo, esta labor deberá ser coordinada con el Administrador de la Red.
- El Administrador de la Red deberá monitorear el desempeño de la red y con base en los resultados deberá planear y ejecutar las mejoras o cambios requeridos para obtener un óptimo desempeño.
- El Administrador de la Red debe evaluar los riesgos asociados con el uso de servicios de red y con base en esto, proponer e implementar los controles requeridos.
- El Administrador de la Red deberá monitorear las conexiones establecidas con redes externas y deberá evaluar los riesgos asociados con estas conexiones. Con base en lo anterior el administrador de la red deberá planear e implementar los controles requeridos.

DIRECTIVA GERENCIAL No. TDD1020

5.6. NORMAS PARA EL USO Y ALMACENAMIENTO DE DATOS E INFORMACIÓN

Uso

Los computadores, servidores y dispositivos periféricos dispuestos y/o entregados por TRANSELCA S.A ESP. a los destinatarios de esta norma, para la ejecución de su objeto social tienen como única y exclusiva finalidad que los mismos sean usados para actividades empresariales. En estos dispositivos solo debe tratarse información empresarial, salvo las excepciones.

Excepciones

De manera excepcional y limitada los destinatarios de esta norma podrán usar y almacenar en el hardware asignado para el desempeño de sus funciones o servicios, archivos relacionados con actividades académicas, información importante concerniente a su núcleo familiar básico, e información personal concerniente con su patrimonio; debiendo en todo caso respetar derechos de terceros. Esta excepción se aplicará de acuerdo al espacio de almacenamiento definido por la Dirección de Gestión de Información conforme las necesidades de cada empleado y/o prestador de servicio.

Esta información será archivada en una carpeta denominada “Información Personal de (nombre del empleado o tercero)”, la cual será creada en cada dispositivo.

El almacenamiento de información diferente a la permitida de manera excepcional, será considerada como una falta disciplinaria y será sancionada de acuerdo a la gravedad del incumplimiento, de acuerdo con la Ley y el Reglamento Interno de Trabajo, en virtud del riesgo potencial que puede derivar para la seguridad de la información de TRANSELCA S.A ESP.

Prohibiciones

Los destinatarios de esta norma no podrán descargar ni almacenar en el hardware entregado por TRANSELCA S.A ESP. información, como fotografías, videos, música (que infrinjan la normatividad en materia de propiedad intelectual y datos personales), juegos, obras multimedia, bases de datos, entre otras, ajenas al desempeño de las funciones contratadas en el marco de relaciones laborales o de prestación de servicios. Lo anterior,

en virtud de que tal acción puede generar un incidente de seguridad sobre los activos empresariales.

Uso de información en hardware propio de los empleados y colaboradores.

TRANSELCA S.A ESP. podrá autorizar a los empleados y colaboradores, cualquiera que sea su vinculación con la empresa, para que puedan utilizar su propio hardware representado en equipos, unidades de disco, entre otros. Atendiendo a que en dicho hardware se gestionará información de esta empresa proveniente del desarrollo de su objeto empresarial y que es obligación de esta empresa custodiar dicha información, los empleados y colaboradores aceptan adoptar y cumplir con las normas expedidas por la empresa para tal efecto, y adoptar las recomendaciones de seguridad informática que determine la Dirección de Gestión de Información, consecuencia de que en sus propios equipos gestionarán información de TRANSELCA S.A ESP. y que bajo este supuesto el hardware queda sujeto a estas normas y directrices. En este caso, entiende el destinatario de esta norma, que la información contenida en dicho dispositivo está sometida a monitoreo y controles en los términos que adelante se expresan.

5.7. CORREO ELECTRÓNICO DE TRANSELCA – CET

Normas Generales

- El uso de identificación de acceso al dominio es personal e intransferible. Esta misma identificación es la que habilita el acceso al CET.
- La definición, modificación o cancelación de las identificaciones de acceso al Correo Electrónico corresponde al Departamento Gestión de la Información, quien está sujeto a lo dispuesto en esta directiva.
- Las comunicaciones internas tales como memorandos, comunicados, notas internas y circulares podrán ser enviados a través del CET; esta comunicación es un documento electrónico reconocido de manera corporativa. Sin embargo las comunicaciones que tengan carácter de comunicación oficial deberán también remitirse al CAD y cumplir con lo definido en el instructivo TIA1004 y en el procedimiento TPA1003.

DIRECTIVA GERENCIAL No. TDD1020

- Se deshabilitará el acceso al CET durante el tiempo que los trabajadores (excepto Gerentes y Jefes de Departamento) estén de vacaciones o suspendidos.
- En el caso de las vacaciones, si se requiere que el trabajador continúe utilizando el CET, el Gerente de Area o Jefe de Departamento deberá solicitar este acceso al Departamento Gestión de la Información, aclarando la necesidad o fin de esta autorización.
- El trabajador deberá hacer uso de este recurso de acuerdo con las normas contenidas en esta directiva. Así mismo la empresa se reserva el derecho de suspender o eliminar el acceso, en el caso que asi lo considere.
- Los usuarios del CET deberán restringir el uso de esta herramienta para el desarrollo de sus labores, de acuerdo con los propósitos definidos en su DRA (Descripción de Responsabilidades Asignadas).
- Los usuarios del CET deberán guardar diligencia y respeto en el contenido de los mensajes enviados, independientemente de a quién (es) sean dirigidos.
- A las listas de distribución oficiales del correo electrónico, tales como, **TRA-Sede Administrativa; TRA-Trabajadores Transelca; Usuarios de Correo de Transelca**, entre otras, únicamente se deben enviar comunicaciones institucionales directamente relacionadas con las responsabilidades asignadas al cargo del empleado que envía el mensaje.
- Para el caso de comités de trabajo, se debe establecer un responsable de las comunicaciones o mensajes de correo electrónico a generar a nombre de dicho comité.
- Cuando se requiera enviar mensajes a las listas de distribución oficiales del correo electrónico con información ajena al objeto social de la empresa, ésta deberá ser remitida a la persona encargada de las comunicaciones del Departamento de Talento Humano, quien será la encargada de enviarla a toda la empresa siempre y cuando esta información esté de acuerdo con las políticas de TRANSELCA S.A. E.S.P.
- El incumplimiento de estas normas, por negligencia o descuido de un usuario acarreará la suspensión temporal o definitiva de su acceso al correo electrónico y TRANSELCA podrá adelantarle un proceso disciplinario por este incumplimiento.

DIRECTIVA GERENCIAL No. TDD1020

Responsabilidades

- Para todos los efectos, el Usuario es el responsable de la utilización de su identificación de correo y deberá observar diligencia y cuidado en el manejo y custodia de la clave asignada.
- Es deber del Usuario evitar que otra persona haga uso de una sesión de correo con su identificación.
- El trabajador es el único responsable de todas las acciones y mensajes que originen y/o remitan con su identificación.
- Las claves o password deberán cambiarse periódicamente por seguridad. El servidor del CET obliga a que la clave de identificación (contraseña) se cambie mínimo cada 30 días.
- Todo nuevo Usuario deberá recibir personalmente su identificación por parte del Dpto. Gestión de la Información y, de inmediato, proceder a cambiar su clave.
- El Departamento Gestión de la Información definirá el tamaño máximo del buzón de los usuarios, quienes serán responsables de la administración racional del espacio asignado a su buzón, teniendo en cuenta que al alcanzar la capacidad máxima definida, el servidor de Correo automáticamente le impedirá enviar nuevos mensajes. Para la información histórica que se requiera almacenar se recomienda a los Usuarios moverla a sus carpetas personales.
- Se debe ser selectivo en cuanto a la información que se envía a través del CET.
- Se debe evitar enviar videos, fotos, sonidos, o cualquier otro archivo de gran tamaño, ya que estos archivos ocupan mucho espacio y congestionan el tráfico en la red. Por lo tanto el Departamento Gestión de la Información definirá un tamaño para los archivos adjuntos a los mensajes que se envíen y reciban.

Prohibiciones

Se prohíbe a los trabajadores de la empresa:

- Usar el Correo Electrónico para propagar mensajes destructivos (virus) u obscenos o de contenido político o religioso.
- Perturbar a los demás usuarios, enviando mensajes que pueden interferir en su trabajo.
- Generar y fomentar el envío de mensajes en cadena.

- Enviar mensajes o documentos utilizando la identificación de otro Usuario.
- Generar o retransmitir comunicaciones de carácter irrespetuoso o que atente contra la integridad de alguna persona, ya sea que se trate de un trabajador de TRANSELCA o no. Usar el correo electrónico para enviar mensajes cuyo contenido lesione a la empresa a los elementos de la Filosofía Corporativa y/o a cualquiera de sus trabajadores.
- Usar el correo electrónico para enviar mensajes cuyo contenido propague actividades que atenten contra la honra y buen nombre de cualquier persona de la organización o fuera de ella.

5.7.1 SUSPENSIÓN DEL SERVICIO POR INCUMPLIMIENTO

Incumplimiento **CORREO ELECTRONICO**	**Suspensión**
Propagar cadenas de mensajes que no tengan que ver con el objeto social de la empresa o al grupo TRANSELCA	Suspensión del servicio de correo por 15 días. Comunicación de la suspensión al Jefe
Enviar mensajes con contenido obsceno o que no contengan código nocivo para la infraestructura informática de la empresa	Suspensión de los servicios de correo e Internet por un (1) mes. Comunicación de la suspensión al Jefe.
Generar o retransmitir comunicaciones de carácter irrespetuoso o que atenten contra la integridad de alguna persona, ya sea que se trate de un trabajador de TRANSELCA o no	Suspensión de los servicios de correo e Internet por término indefinido. Comunicación de la suspensión al Jefe.
Enviar a las listas de distribución oficiales del correo electrónico, tales como, TRA-Sede Administrativa; TRA-Trabajadores Transelca; Usuarios de Correo de Transelca, entre otras, información ajena al objeto social de TRANSELCA, sin la coordinación del Departamento de Talento Humano.	Suspensión de los servicios de correo e Internet por 15 días. Comunicación de la suspensión al Jefe.
Usar el correo electrónico para enviar mensajes cuyo contenido lesione a la empresa, o sus elementos de Filosofía Corporativa y/o a cualquiera de sus empleados	Suspensión de los servicios de correo e Internet por término indefinido. Comunicación de la suspensión al Jefe.

El uso indebido del CET y de acuerdo a la gravedad de la falta o casos de reincidencia, TRANSELCA S.A. E.S.P, a través del Comité de Seguridad Informática, podrá aplicar sanciones y/o realizar procesos disciplinarios según lo establecido en la Convención Colectiva del Trabajo y en la Legislación Colombiana.

5.8 ACCESO A INTERNET

TRANSELCA S.A. E.S.P., ofrece a sus colaboradores el acceso a Internet, como herramienta para el óptimo desempeño de sus labores. Este es un servicio que se da a través del acceso al dominio.

Normas Generales

- Cuando se le solicita acceso a la red a un trabajador o a un colaborador, de acuerdo al Instructivo TIA5004, se crea un usuario, y con base en lo solicitado por su jefe se le habilita el acceso de navegación en internet a través del acceso al dominio.
- La definición, modificación o cancelación de las identificaciones de acceso al Dominio corresponde al Administrador de Usuarios, de acuerdo a lo solicitado por los Jefes y los Gerentes y según lo definido en la Directiva.
- El uso de la identificación de acceso al Dominio es personal e intransferible. Esta identificación es la que habilita el acceso a Internet.
- Se deshabilitará el acceso al dominio durante el tiempo que los trabajadores (excepto Gerentes y Jefes de Departamento) estén disfrutando de sus vacaciones o suspendidos.
- En el caso de las vacaciones, si se requiere que el trabajador continúe accesando al dominio, el Gerente de Área o Jefe de Departamento deberá solicitar este acceso al Departamento Gestión de la Información, aclarando la necesidad o fin de esta autorización.
- El acceso a Internet es un servicio para el desarrollo de las labores de los usuarios de acuerdo con los propósitos definidos en su DRA – Descripción de Responsabilidades Asignadas. No obstante, se podrá utilizar el servicio de Internet para actividades personales de acuerdo a las restricciones impuestas por la compañía en relación con los horarios y tiempos de utilización y sitios a consultar.

Transelca se reserva el derecho de restringir el acceso a Internet para actividades personales.

- El Departamento Gestión de la Información podrá llevar registros y estadísticas del uso de Internet, incluyendo identificación del usuario, horario y sitios de navegación.
- Los usuarios del servicio de Internet también deberán guardar diligencia y respeto en el contenido de los mensajes enviados a través de internet, desde los sistemas de mensajería diferentes al CET independientemente de a quién (es) sean dirigidos.
- El incumplimiento de estas normas, por negligencia o descuido de un usuario, acarreará la suspensión temporal o definitiva del servicio.

Responsabilidades

- Para todos los efectos, el usuario es el responsable de la utilización de su identificación de acceso al Dominio y deberá observar diligencia y cuidado en el manejo y custodia de la clave asignada.
- Es deber del Usuario evitar que otra persona use su identificación para acceso a los servicios de la Red Corporativa, en este caso en particular para el acceso a Internet.
- El trabajador es el único responsable de todas las acciones que se originen y/o remitan con su identificación, incluyendo envío de mensajes (dañinos, obscenos o que atenten contra la integridad de alguna persona u organización), desde sitios de correo gratuito.
- La clave de la identificación de acceso a la red deberá cambiarse periódicamente por seguridad. El servidor del dominio obliga a que la clave de identificación (contraseña) se cambie mínimo cada 30 días.
- Se debe ser selectivo con los sitios de navegación en Internet. Es importante seguir las recomendaciones del Departamento Gestión de la Información al respecto, pues muchos virus informáticos, códigos maliciosos y páginas de publicidad no solicitadas son transmitidas por este medio.
- La descarga de software desde Internet por parte de los usuarios deberá ser coordinada previamente con el Departamento Gestión de la Información. Bajo ningún caso
  se podrá descargar software para el cual TRANSELCA no posea licencia de uso.

- La instalación del software en los computadores de la Empresa está reglamentada en el Capítulo 9 “Cumplimiento de Políticas y Normatividad Legal y en el Numeral 5.8 Políticas de Computadores Personales y en la Política de Ética.
- El incumplimiento de estas Normas, por negligencia o descuido de un usuario acarreará la suspensión temporal o definitiva del servicio.

Prohibiciones

Se prohíbe a los trabajadores de la empresa usar el acceso a Internet para:

- Descargar programas destructivos u obscenos
- Atentar contra la integridad de alguna persona u organización, ya sea que se trate de un trabajador de TRANSELCA o no.
- Propiciar el envío de cadenas de correo.
- Utilizar sistemas de mensajería de internet diferentes al CET para generar o retransmitir comunicaciones de carácter irrespetuoso o que atenten contra la integridad de alguna persona, ya sea que se trate de un trabajador de TRANSELCA o no, o para enviar mensajes cuyo contenido lesione a la empresa, a los elementos de la Filosofía Corporativa y/o a cualquiera de sus empleados.

5.8.1 SUSPENSIÓN DEL SERVICIO POR INCUMPLIMIENTO

Incumplimiento	**Suspensión**
ACCESO A INTERNET	
Utilizar servicios de correo gratuitos para enviar mensajes: ➢ Que atenten contra la integridad de alguna persona ➢ Que contenga código nocivo para la infraestructura informática de la empresa	Suspensión de los servicios de correo e Internet por término indefinido. Comunicación de la suspensión al Jefe y copia a la hoja de vida

DIRECTIVA GERENCIAL No. TDD1020

Incumplimiento	Suspensión
ACCESO A INTERNET	
Utilizar servicios de correo gratuitos para enviar a las listas de distribución oficiales del correo electrónico, tales como, TRA-Sede Administrativa; TRA-Trabajadores Transelca; Usuarios de Correo de Transelca, entre otras, información ajena al objeto social de TRANSELCA, sin la coordinación del Departamento de Talento Humano.	Suspensión de los servicios de correo e Internet por 15 días. Comunicación de la suspensión al Jefe.
Afectar el rendimiento de la red corporativa y/o el canal de acceso a Internet, debido al uso irracional de este recurso	Suspensión del servicio de acceso a Internet por un mes. Comunicación de la suspensión al Jefe
Está prohibido establecer sesiones de chat's, transmisión de videos y/o descargas de música para desarrollar actividades ajenas al objeto social de TRANSELCA S.A. E.S.P.	Suspensión del servicio de acceso a Internet por un mes. Comunicación de la suspensión al Jefe
Utilizar sistemas de mensajería de Internet diferentes al CET para generar o retransmitir comunicaciones de carácter irrespetuoso o que atenten contra la integridad de alguna persona, ya sea que se trate de un trabajador de TRANSELCA o no, o para enviar mensajes cuyo contenido lesione a la empresa a los elementos de la Filosofía Corporativa y/o cualquiera de sus empleados	Suspensión de los servicios de correo e Internet por término indefinido. Comunicación de la suspensión al Jefe y copia a la hoja de vida.

El uso indebido del servicio de acceso a Internet y de acuerdo a la gravedad de la falta o casos de reincidencia, TRANSELCA S.A. E.S.P, a través del Comité de Seguridad Informática, podrá aplicar sanciones y/o realizar procesos disciplinarios según lo establecido en la Convención Colectiva del Trabajo y en la Legislación Colombiana.

5.8.2 OTRAS SUSPENSIONES

Acceso a los Sistemas de Información y Otros Servicios de la Red	**Suspensión**	**Comentarios**
Usar la identificación de otra persona sin consentimiento del dueño de la identificación	Suspensión del acceso al servicio por término indefinido.	
INSTALACIÓN DE SOFTWARE		
Instalar software sin la autorización o coordinación con el Departamento Gestión de la Información	Suspensión del acceso al servicio por término indefinido. Comunicación de la sanción al Jefe	Esta falta es considerada grave por ser de cumplimiento legal.

De acuerdo a la gravedad de la falta o casos de reincidencia, TRANSELCA S.A. E.S.P. podrá realizar procesos disciplinarios, según lo establecido en la Convención Colectiva del Trabajo y en la Legislación Colombiana.

5.9. POLÍTICAS DE COMPUTADORES PERSONALES (INCLUYE COMPUTADORES PORTÁTILES)

La empresa ofrece a sus colaboradores, para el óptimo desempeño de sus labores, las herramientas informáticas requeridas, como computadores personales o estaciones de trabajo. En este aspecto se ha definido lo siguiente:

- Los computadores personales, su tipo, características y accesorios serán asignados según la labor a desempeñar por los Usuarios.
- Los Jefes de Departamento solicitarán al Departamento Gestión de la Información la asignación o intercambio de los computadores personales del personal a su cargo, de acuerdo con las recomendaciones del Departamento Gestión de la Información.

DIRECTIVA GERENCIAL No. TDD1020

- El Departamento Gestión de la Información debe mantener un inventario del hardware y software que componen cada uno de los computadores personales, relacionando el (los) usuario(s) responsable(s) de su custodia.
- Los Usuarios deberán cuidar y proteger los equipos informáticos a su cargo, utilizándolos de una manera adecuada y eficiente para el desarrollo de las labores que les asignó la empresa.
- Los computadores personales deben poseer tecnología actualizada, procurando su renovación por lo menos cada cinco años.
- La Mesa de Ayuda del Departamento de Gestión de la Información (Línea 73000) es la encargada de configurar e instalar el hardware y el software que se requiera. Antes de instalar cualquier software, deberá verificar que TRANSELCA posea su licencia de uso.
- Si el Usuario requiere algún software o hardware adicional al instalado en la estación de trabajo, su Jefe Inmediato debe solicitarlo al Departamento Gestión de la Información, quien evaluará técnicamente el requerimiento y procederá a adquirirlo e instalarlo. Si se requiere un software adicional, se deberá revisar la disponibilidad de la licencia de uso. En caso de no poseerla el Departamento Gestión de la Información deberá adquirirse la licencia previamente a la instalación del software.
- Los Usuarios de los computadores personales deberán conocer y cumplir las políticas de uso de los recursos informáticos.
- Los Gerentes, Directores o Jefes de Departamento serán los responsables de los computadores personales de los Contratistas y Estudiantes en Entrenamiento de su área.
- Si un trabajador desea retirar un computador o cualquier accesorio informático de la sede de la empresa, debe ser autorizado por el Jefe del Departamento Gestión de la Información o el Coordinador de Computadores (Especialista en Informática), mediante la firma de los formatos Autorización de Salida de Elementos y/o Materiales, el cual debe ser presentado a la salida de la sede para que el Guardia de la recepción lo registre y anote su número de serie, de acuerdo con lo definido en el Procedimiento Ingreso y Salida de Personas y Materiales de las Sedes de TRANSELCA - TPA1002.
- En el evento en que el empleado que desee retirar un computador portátil de la sede de la empresa, sea el custodio del mismo, no tendrá que diligenciar ningún

formato de autorización, pero el Guardia de la recepción verificará que la persona que lo retira es la responsable del mismo, consultando y registrando el retiro del equipo en el aplicativo de Control de Equipos de TI.

5.10. NORMAS PARA LA REALIZACIÓN DE TRABAJOS EN CASA

- Cuando se requiera trasladar un equipo portátil o medios magnéticos fuera de la sede la empresa para realizar trabajos en casa, es responsabilidad del trabajador el cuidado y protección del equipo u otro.
- El Usuario deberá controlar el acceso a los recursos, asegurando la información confidencial de accesos no autorizados.
- No se deben realizar copias de información sensible en equipos que no sean propiedad de la empresa. En caso de que sea absolutamente necesario, se deberá destruir estas copias en cuanto ya no sea requerida la información.

CAPÍTULO 6. SISTEMA DE CONTROL DE ACCESO Y SEGURIDAD LOGICA

6.1. CONTROLES DE ACCESO

- La Gerencia Dueña de la Información debe otorgar los accesos a datos y servicios
- TI, de acuerdo con las políticas de acceso del negocio, es decir, se debe brindar acceso a los Usuarios únicamente a servicios requeridos para el desempeño de sus labores.
- El Usuario dueño de la información debe cumplir con las normas para el control de la asignación de derechos de acceso a Usuarios, incluyendo todas las etapas del ciclo de vida del Usuario, desde su registro inicial hasta la eliminación del registro a quienes no necesiten más acceso.
- En conjunto, el Dueño y el Custodio de la Información deberán establecer un proceso para monitorear el acceso y uso del sistema.

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

6.2. MANEJO DE LOS ACCESOS A LOS SISTEMAS COMPUTACIONALES

Responsabilidades

- El uso de las claves de acceso (contraseñas) a los Sistemas de Información es personal e intransferible.
- El Usuario es el responsable de la utilización de las identificaciones y contraseñas asignadas a él para el acceso a los diferentes Sistemas de Información; por lo tanto, deberá observar diligencia y cuidado en el manejo y custodia de las mismas.
- Es deber del Usuario evitar que otra persona haga uso de sus identificaciones y contraseñas para acceder cualquiera de los Sistemas de Información de TRANSELCA y será responsable por el acceso a estos y por las autorizaciones y aprobaciones asignadas a su identificación.
- La definición, modificación o cancelación de las identificaciones de acceso, corresponde al Departamento Custodio del Sistema quien se sujetará a lo dispuesto en la presente Directiva Gerencial.

Normas para el Manejo de las Claves de Acceso

1. Todo nuevo Usuario deberá recibir personalmente su identificación y contraseña por parte del Departamento Custodio del Sistema y, de inmediato, deberá proceder a cambiarla.
2. Por motivos de seguridad, la contraseña de la identificación deberá cambiarse periódicamente mínimo cada 30 días, lo cual será exigido por el sistema.
3. La longitud mínima permitida para la contraseña es de mínimo 8 caracteres, los cuales deben ser combinaciones de números, letras y caracteres especiales.
4. Las últimas tres contraseñas utilizadas por el Usuario serán registradas por los sistemas de información y no podrán reutilizarse.
5. Después de tres intentos fallidos de acceso a cualquiera de los Sistemas de Información, utilizando una clave errónea, automáticamente se bloqueará el acceso posterior a este sistema. Para una nueva habilitación, el Usuario deberá comunicarse con el Departamento Custodio del Sistema ó con la Mesa de Ayuda (Línea 73000) ó utilizando las funcionalidades dispuestas para el desbloqueo de claves.

Los ítems 2, 4 y 5 se excluyen para el Sistema SCADA, dado que la filosofía de funcionamiento del mismo no permite tales características de forma automática.

Administración de Claves de Superusuarios

- Las claves de los Superusuarios deben cumplir con las normas definidas para los controles de acceso de los sistemas computacionales.
- Como medida de protección, los administradores de los servidores deben utilizar un usuario privilegiado para sus labores, diferente al que utilizan como usuario administrador estándar.
- Por cada usuario administrador debe existir un usuario diferente pero con los mismos privilegios, el cual debe ser manejado por el administrador de respaldo asignado.

6.3. SEGURIDAD LOGICA

- En TRANSELCA las aprobaciones electrónicas que se realizan a través de los sistemas son tan válidas como la aprobación con una firma.
- Es responsabilidad de los trabajadores proteger la información confidencial de la empresa, por lo tanto los Usuarios deben definir y aplicar controles de acceso a los archivos electrónicos que contengan información confidencial.
- En caso de que un Usuario requiera compartir con otros Usuarios alguna de la información almacenada en su computador personal, es responsabilidad del Usuario aplicar medidas de seguridad que habilitará en su computador para el acceso a la información.
- Si un Usuario necesita compartir a toda la empresa información que se encuentra en medio electrónico, deberá solicitar su publicación en la Intranet.

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

CAPÍTULO 7. MANTENIMIENTO Y DESARROLLO DE SISTEMAS Y OTRAS HERRAMIENTAS DE SOFTWARE

Para minimizar los riesgos de seguridad en las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información se definió lo siguiente:

- El Departamento Custodio del Sistema de Información velará porque el sistema de información respectivo posea ambientes separados para producción y para desarrollo, pruebas y entrenamiento.
- El Administrador del Sistema de Información debe asegurar que los requerimientos y criterios de aceptación de un nuevo sistema se definan claramente, se acuerden, documenten y prueben por parte de los proveedores y los Usuarios de la aplicación.
- El Administrador del Sistema debe identificar los requerimientos de seguridad durante la etapa de requerimientos. Adicionalmente para la selección de un Sistema ya desarrollado se debe tener en cuenta los aspectos de seguridad definidos.
- El Departamento Custodio del Sistema exigirá la aplicación de las políticas de seguridad establecidas a todo proyecto de Tecnología Informática.
- El Departamento Custodio del Sistema velará por existencia de instructivos actualizados para la operación del respectivo sistema de TI.
- El Administrador del Sistema es responsable de coordinar que se realice el entrenamiento a los Usuarios en el uso de sistema, antes de implantar una nueva aplicación.
- El Usuario líder debe validar, al momento de recibo de la aplicación o de las actualizaciones, la información procesada por los programas de aplicación.
- El Departamento Custodio del Sistema velará porque exista un control estricto en la implementación de cambios.
- El Administrador del Sistema debe cerciorarse que el Usuario líder dé su aprobación del cambio, previamente a la actualización de la aplicación.
- Después de la aprobación de un cambio en el sistema por parte del Usuario líder del mismo, es su responsabilidad el correcto funcionamiento de la nueva aplicación.
- Los datos de prueba deben ser protegidos, controlados y documentados.
- Cuando deban realizarse cambios en los sistemas operativos, el Administrador del Servidor debe seguir un procedimiento documentado y debe revisar el impacto en la seguridad del sistema.

DIRECTIVA GERENCIAL No. TDD1020

Responsabilidad para la actualización de herramientas de software

- La actualización de las herramientas tecnológicas que hacen parte de la plataforma corporativa, tales como OFFICE, SAP, antivirus, sistemas de mensajería electrónica y colaboración, sistemas operativos, Laser Fiche, entre otras, son responsabilidad del
- Departamento Gestión de la Información, quien definirá los ciclos de renovación de acuerdo con las políticas establecidas.
- La actualización de herramientas tecnológicas especializadas asignadas a áreas o usuarios específicos, tales como: Autocad, ACL, MathCad, Digsilent, , entre otros, deben ser solicitadas y justificadas por los Departamentos usuarios de estas tecnologías para que sean adicionadas por el Departamento Gestión de la Información en el presupuesto del siguiente período. La implementación de estas actualizaciones se realizarán en forma coordinada entre el Departamento Gestión de la Información y los Departamentos usuarios.

CAPÍTULO 8. PLANES DE CONTINGENCIA

Con el fin de prepararse para la interrupción de las actividades del negocio, se ha definido lo siguiente:

- El plan de contingencia debe incluir los procedimientos apropiados de recuperación para los procesos y servicios esenciales, con el fin de que estos sean restaurados y mantenidos lo más pronto posible.
- Para que un plan de contingencia sea exitoso, toda la información sensible, valiosa o crítica residente en los sistemas de cómputo de la empresa debe respaldarse periódicamente.
- El Dueño del Sistema de Información debe especificar los marcos de tiempo mínimos aceptables y los tipos de datos que necesitan ser respaldados, para una eventual contingencia.
- El Dueño del Sistema de Información debe definir las categorías de criticidad para la información, de tal forma que las aplicaciones más críticas reciban especial atención durante el desarrollo de los planes de contingencia.

- El Departamento Custodio del Sistema, de acuerdo con la información presentada por el Dueño del Sistema de Información, debe asignar una prioridad a cada uno de los procesos y servicios esenciales, con el fin de que estos sean recuperados de acuerdo a la criticidad de cada servicio.
- Los planes de contingencia deben ser probados, revisados y actualizados cada que se presenten cambios en la infraestructura del servicio o por otras necesidades que se detecten, .

CAPÍTULO 9. CUMPLIMIENTO DE POLÍTICAS Y NORMATIVIDAD LEGAL

La empresa en desarrollo de la política de tener la totalidad del software legalizado, y de acuerdo con la Ley 44 de 1993 – Derechos de Autor -, definió los siguientes aspectos para la utilización e instalación de software los cuales se detallan en el Instructivo TIA5005.

- Todo el software instalado en los computadores de la empresa debe poseer licencia vigente de uso.
- En ningún caso se autorizará la instalación de software en los computadores de la empresa, si anteriormente no se ha adquirido la licencia de uso o no se ha recibido permiso escrito por parte del dueño de los derechos de autor del software.
- El Departamento de Gestión de la Información será responsable de fomentar la cultura de utilización de software legal dentro de los Usuarios de computadores personales de la empresa.
- Cuando exista necesidad de uso de un software especial, el jefe de Departamento del usuario que lo requiera lo debe solicitar al Departamento Gestión de la Información. El Departamento Gestión de la Información verificará la viabilidad técnica y coordinará la instalación y la adquisición del software, si es el caso, de acuerdo a los requerimientos del Usuario y de la empresa.
- El software desarrollado por trabajadores o Contratistas de la empresa, es de total propiedad de TRANSELCA y se debe respetar la propiedad intelectual.
- En los servidores y computadores de propiedad de TRANSELCA se podrá instalar software licenciado a título personal, siempre y cuando se ajuste a lo establecido en el Instructivo TIA5005.
- El Departamento Gestión de la Información debe asegurar que los documentos que respaldan la instalación de software en los computadores y servidores asociados,

deben reposar en un sitio centralizado y seguro de la empresa, que posea controles de acceso y ambientales.

- Es deber del Departamento Gestión de la Información administrar las licencias del software instalado en la empresa, manteniendo actualizado el inventario de software instalado y de licencias adquiridas.
- Cuando se requiera instalar software libre de uso en los computadores de la empresa, el Jefe del Departamento que tiene la necesidad deberá solicitarlo al Departamento Gestión de la Información, adjuntando la licencia de uso en la que el dueño de los derechos de autor exprese que autoriza su libre uso a organizaciones o entidades de la naturaleza de TRANSELCA. El Departamento Gestión de la Información entregará computadores personales a los colaboradores de la empresa, como parte de sus herramientas de trabajo. Al recibirse el computador se deberá firmar el acta de recibo en la cual, el custodio se compromete a no instalar software en ese equipo y a cumplir con las políticas de Seguridad Informática.
- Las licencias de software, instaladores de software deben ubicarse en un sitio que posea control de acceso y de temperatura.
- Cualquier incumplimiento de lo enunciado en esta política, se considerará como una falta grave y podrá adelantarse un proceso disciplinario en contra de los trabajadores y/o terceros que hayan incurrido en la falta.

Los lineamientos, normas y demás instrucciones contenidas en esta directiva, son de obligatorio cumplimiento en TRANSELCA.

4. DOCUMENTOS DE REFERENCIA

- Modelo Normativo de Seguridad del Sistema Aplicativo SAP.
  http://extranetgrupo.isa.com.co/ModeloNormSegSAP.htm

- Guía para el uso y la gestión de la tecnología de la información – Guía Institucional No 4
  http://extranetgrupo.isa.com.co/guiaGestion.htm

5. CONTROL DE REGISTROS

Código del Registro o Identificación	Nombre del Registro	Responsable del Registro	Archivo o Almacenamiento	Tiempo de Retención
N.A.	N.A.	N.A.	N.A.	N.A.

6. RELACIÓN DE CAMBIOS

Actualización No.	Cambios	Descripción de los Cambios	Fecha de la Última Revisión	Revisado por	Aprobado por
00	Se modificó la conformación del Comité de Seguridad Informática	Se incluyó al Jefe del Dpto de Telemática y a un Representante de la Gerencia de Transmisión	22 de Mayo de 2001	Jefe Dpto Informática Jefe Dpto Telemática	Gerente General
	Se amplió a todas las áreas que son custodios de Sistemas de Información, las responsabilidades del Comité de Seguridad Informática	Se definieron como responsabilidades para todas las áreas que son custodios de Sistemas de información, las responsabilidades definidas por el Comité de Seguridad Informática			
	Se modificaron las responsabilidades del Comité de Seguridad Informática	Se definió que el Comité de Seguridad Informática definiera las políticas generales para la seguridad de los sistemas			

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

00	Los correspondientes a lo definido en el Instructivo para la edición y codificación de Manuales de Macroprocesos, Directivas Gerenciales, Procedimientos e Instructivos TID1001	➢ El código ahora es TDD1020. ➢ Las definiciones se encuentran en el Diccionario Corporativo ➢ Se adicionó el Control de Registros y la Relación de Cambios como parte del Procedimiento	22 de Mayo de 2001	Jefe Dpto Informática Jefe Dpto Telemática	Gerente General
	Especificaciones del manejo de medios de tomas de respaldo	➢ Se describe la programación definida para el envío de los medios que contienen las copias de respaldo a un sitio alterno			
	Instructivo de Administración y Registro de accesos a los Sistemas de Información	➢ Se precisó cómo debe realizarse la solicitud de acceso a la red que apoya la gestión administrativa de todos los macroprocesos de la compañía.			

00	Referencia al TIA1004 y al TPA1003	➢ Se hace referencia al Instructivo TIA1004 y al Procedimiento TPA1003, para la utilización del Correo Electrónico CET-	22 de Mayo de 2001	Jefe Dpto Informática Jefe Dpto Telemática	Gerente General
	Precisión de políticas específicas del Correo Electrónico – CET -	➢ Se precisaron algunas políticas específicas del Correo Electrónico – CET- como las referentes al tamaño del buzón y de los archivos adjuntos			

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

	Modificación al Plan de Continuidad del Negocio por Planes de Contingencia	➢ Modificación del esquema de respaldo del Plan de Continuidad del Negocio por Planes de Contingencia			
	Condiciones físicas para equipos críticos de los sistemas	➢ Se incluyeron los demás equipos críticos de los sistemas dentro de las mismas condiciones físicas de los servidores			
	Responsabilidad de proveer herramientas de informática a los trabajadores de la compañía	➢ Se amplió a las otras áreas que son custodia de los sistemas de información, las responsabilidade proveer herramientas de informática a los trabajadores de la compañía.			

01	Modificación a la periodicidad de reunión del comité de Seguridad Informática.	➢ Se definió que el comité se reunirá como mínimo dos veces al año.	20 de Noviembre de 2002	Jefe Dpto. Informática Jefe Dpto. Telemática	Gerente General
	Modificación a la longitud de las claves de acceso a los Sistemas	➢ Se modifica la longitud de la clave de 6 a 7 caracteres			
	Definición del alcance de las Normas para el manejo del las claves de acceso	➢ Se definió la aplicabilidad de las normas para el manejo de las claves de acceso para el Sistema SCADA.			

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

02	Cambio en el Capítulo 1 y adición del punto 5.10 “Acceso a Internet”	➢ Se suprimió el número de veces para realizar reuniones del Comité de Seguridad Informática” y ➢ Se agregó el punto 5.10 “Acceso a Internet” (Normas Generales), Responsabilidades y Prohibiciones)	1 de Diciembre de 2003	Jefe Dpto. Informática	Gerente General
02	No Registra	No Registra	No Registra	No Registra	No Registra

03	Cambio en el texto de la Política Numeral 2 y en los Capítulos 5 en los numerales 5.7 y 5.8 y Capítulo No. 9	➢ Modificación en el texto de la Política ➢ Cambio en las Normas Generales y en las Prohibiciones. Adición del punto 5.7.1 “Suspensión del Servicio por Incumplimiento” ➢ Modificación en las Normas Generales, Responsabilidades y Prohibiciones y adición del punto 5.8.1 “Suspensión del Servicio por Incumplimiento” y “Otras Suspensiones” ➢ Modificación del texto en el Capítulo 9 “Cumplimiento de Políticas y Normatividad Vigente”	8 de Septiembre de 2004	Jefe Dpto de Informática	Gerente General

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

04	Cambios generales en el documento	➢ Se modifica de acuerdo al nivel de responsabilidad, dueños y custodios y homologando los procesos implementados en la compañía y además teniendo en cuenta la plataforma tecnológica implementada en la empresa. ➢ Se cambian los términos “Compañía” por “Empresa” y “Clientes” por “Usuarios”. ➢ Se establecieron precisiones en el sentido de envíos de correos a los Buzones Oficiales de TRANSELCA.	Jefe Departamento Informática	Gerente General	

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

05	Cambio en los capítulos 1,5 y7	Se modifica en el capítulo 1, delegar en el Dpto. de Recursos Humanos enviar memorando al trabajador que viole lo establecido en la Directiva TDD1020. En el capítulo 5 se adiciona la regulación en el almacenamiento de archivos personales en los recursos de la empresa y el uso del internet en actividades personales, según las restricciones de la empresa para los trabajadores, contratistas o estudiantes en práctica que violen lo establecido en la Directiva. En el título de las Prohibiciones se elimina. “La prohibición para establecer sesiones de Chat’s, transmisión de videos y/o descargas de música para desarrollar actividades ajenas al objeto social de TRANSELCA S.A. E.S.P.” De igual manera en el capítulo 7 se adiciona la responsabilidad para la actualización de herramientas de Software.	3 de Abril de 2008	Jefe Dpto. Informática	Gerente General

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

06	Se adiciono el inciso 4: “Documentos de Referencia”	Se adicionó este inciso para hacer referencia a los siguientes documentos de grupo: • Modelo Normativo de Seguridad del Sistema Aplicativo SAP R/3 • Guía para el uso y la gestión de la tecnología de la información	2 de Enero de 2009	Jefe Dpto. Informática	Gerente General
07	Se cambió la codificación de los procedimientos e instructivos a los que hacía referencia la directiva.	Se cambiaron las codificaciones de TIO3016, TIO3019 y TIO3036 por TIA5001, TIA5004 y TIA5005, respectivamente.	13 de Marzo de 2009	Jefe Dpto. Informática	Gerente General
08	Se homologaron conceptos con la Política de Información y del Conocimiento	Los conceptos de Información Confidencial y Publica fue homologada con la Política de Información y del Conocimiento del Grupo Empresaria ISA	16 de Julio de 2010	Jefe Dpto. Informática	Gerente General
09	No Registra	No Registra	No Registra	No Registra	No Registra
10	Modificaciones al capítulo 3: Seguridad con el personal.	Cambios en el compromiso relacionado con la educación en seguridad informática para los empleados y contratistas, reemplazándola por el compromiso de divulgación de normas de la directiva.	24 de Septiembre de 2010	Jefe Dpto. Informática	Gerente General

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

11	Modificación en el capítulo 8: Planes de Contingencia	Se indica que los planes de contingencia se prueban, revisan y actualizan por cambios en la infraestructura del servicio o por necesidades que se detecten.	12 de Septiembre de 2011	Jefe Dpto. Informática	Gerente General
12	Modificación en el numeral 5.7 Correo Electrónico, y numeral 5.8 Acceso a Internet	➢ En esta modificación se define cómo habilitar el acceso al correo electrónico a los trabajadores en permiso sindical permanente. ➢ En esta modificación se define cómo habilitar el acceso a Internet a los trabajadores en permiso sindical permanente.	13 de Agosto de 2012	Jefe Dpto. Informática	Gerente General
13	Modificación en el numeral 5.2	-Cambio nombre de numeral: "Manejo de Medios de Respaldo" por "Politica de Respaldo y Recuperacion de Informacion" -Adición de parrrafo sobre "la programación de pruebas aleatorias a los medios de respaldo"	07 de Marzo de 2014	Jefe Dpto. Informática	Gerente General
	Modificacion en el numeral 5.8.1	Cambio en encabezado de tablas: "Corre electrónico" por Acceso a Internet"			

TRANSELCA

DIRECTIVA GERENCIAL No. TDD1020

	Modificacion en el numeral 5.9	Cambio de palabra “helpdesk” por “Mesa de Ayuda”. Adición a párrafo sobre retiro de computador portátil.			
	Modificacion en el numeral 6.2	Modificación de la parte 5 sobre Normas para el Manejo de las Claves de Acceso			
	Modificación al numeral 1.1 sobre el Comité de Seguridad Informática	Retiro del Jefe del Departamento Gestión Operativa del Comité de Seguridad Informática Se incluye un representante de Secretaría General al Comité de Seguridad Informática			
14	Cambios en el nombre del Departamento de Informática y Recursos Humanos	Se actualizó el nombre del Departamento de Informática a Departamento de Gestión de la Información. Se actualizo el nombre de Departamento de Recursos Humanos a Talento Humano.	16 de Mayo de 2014	Jefe Dpto. Gestión de la Información	Gerente General
15	Modificacion en el numeral 5.6	Se modifica el numeral para definir el uso , las expeciones y prhobicione en el almacenamiento de datos e informacion.	22 de Abril 2015	Dirección Gestión de la información	Gerente General