

1. OBJETIVO

Dar cumplimiento a la normatividad legal vigente, y con el fin de mantener la Integridad, disponibilidad, confidencialidad, autenticidad y autoría de cambios en los sistemas de información, servicios de red y recursos informáticos de la Empresa. Establecer medidas de control para el buen uso de los accesos a sistemas de información, servicios de red, copias de seguridad y demás componentes tecnológicos de **TERMINAL DE TRANSPORTES DE IBAGUÉ S.A.**

2. ALCANCE

Toda persona vinculada como funcionario o contratista a **TERMINAL DE TRANSPORTES DE IBAGUÉ S.A.**, se compromete a:

- Guardar confidencialidad de la información que conozca en el desempeño de sus funciones tal como información personal de clientes, empleados, accionistas, afiliados, proveedores y/o cualquier información considerada como confidencial para la empresa.
- Acatar las directrices de la Política de Seguridad informática, cumplir los procedimientos e instructivos que le den despliegue a la misma.

3. POLÍTICAS ESPECÍFICAS

Se establecen las siguientes políticas de obligatorio conocimiento y cumplimiento:

3.1. REGISTRO Y ACCESO

- Cada funcionario o contratista de la Empresa que tenga acceso a los sistemas de información, servicios de red de la Empresa tendrá asignado un identificador o nombre de usuario personal e intransferible y una contraseña de autenticación.

- Toda solicitud de acceso a sistemas de información y/o servicios de red deberá ser solicitada formalmente por un rol directivo relacionando el perfil, atribuciones, restricciones y vigencia del acceso solicitado.
- Los identificadores o cuentas de acceso tendrán vigencia de acuerdo con la solicitud o mientras exista el vínculo contractual con la Empresa.
- Para evitar el uso no autorizado y/o suplantación de identidad en los sistemas de información, los empleados y/o responsables de equipos de cómputo deberán garantizar el bloqueo en caso de ausencia del puesto de trabajo obligando la digitación de la contraseña antes de poder utilizarlo nuevamente.
- Está prohibida la divulgación por cualquier medio escrito, electrónico o verbal de las contraseñas asignadas. Es responsabilidad de cada usuario su conocimiento y custodia, ya que estas garantizan su identificación y autoría en la generación y/o modificación de la información.
- Ante el olvido de su contraseña por parte de un usuario se deberá solicitar formalmente al Coordinador de Sistemas, la asignación de una nueva contraseña obligando a su cambio en su primer uso.
- Los funcionarios deberán abstenerse de intentar acezar sistemas de información y servicios de red mediante el uso de credenciales no asignadas, suplantación, fraude o técnicas de fuerza bruta que comprometan la disponibilidad del servicio o sistema.
- Los jefes de proceso podrán solicitar formalmente al Coordinador de Sistemas el cambio de contraseñas para accesos a sistemas de información y servicios de red de personal a su cargo con el fin de garantizar disponibilidad y confidencialidad de la información de sus procesos.
- El Coordinador de Sistemas podrá implementar controles de bloqueo automático, al alcanzar cierto tiempo de inactividad en la sesión del sistema o servicio.
- Los sistemas de información que registren contraseñas de autenticación deberán ser almacenadas en formato encriptado de tal forma que ningún usuario, sin importar su perfil pueda visualizarlas.

3.2. DATOS PERSONALES

- Los funcionarios deben acatar las políticas de tratamiento de datos personales particulares de cada base de datos y en específicamente la finalidad con que fue recaudada dichos datos.
- Los funcionarios deben abstenerse de exceder sus responsabilidades sobre datos personales al extraer, copiar, duplicar, compartir, transferir, almacenar información de datos personales de los sistemas de información de la empresa.
- Los funcionarios que deban transferir información a la que tenga acceso por motivos de sus funciones relacionadas con el tratamiento de datos, deberán tomar las precauciones necesarias para evitar la pérdida de confidencialidad, integridad y disponibilidad de la información a transferir.

- Los funcionarios son responsables de reportar al oficial de protección de datos personales cualquier incidente, novedad o riesgo de confidencialidad, integridad o disponibilidad de datos personales en bases de datos de la empresa.

3.3. INTERNET

- Está prohibido el acceso a páginas con contenidos ilícitos, material pornográfico, de contenido racista, sexual, o cualquier material que atente contra la dignidad y los principios morales.
- El servicio de Internet podrá filtrar los accesos a los sitios que a consideración del Gerente o del Coordinador de sistemas sean inapropiados para la empresa, o innecesarios para la actividad laboral.
- Queda prohibida la utilización del servicio de internet para navegar por sitios de Internet para usos que no sean relacionados para el desempeño de las funciones.

3.4. CORREO ELECTRÓNICO

- Todo funcionario que requiera el uso de un buzón de correo electrónico para generar o recibir comunicaciones a nombre de la organización, deberá utilizar una cuenta de correo creada bajo el dominio de **terminalibague.com**, la que le será entregada junto con su clave personal.
- El identificador de cuenta será impersonal y corporativo; en casos excepcionales será personalizada a solicitud formal y justificada por un rol directivo.
- Cuando el funcionario se retire de la empresa su cuenta de correo será inactivada y la contraseña cambiada para inhabilitar el acceso del funcionario desvinculado.
- El correo electrónico del Terminal de Transportes de Ibagué es entregado sólo para uso en asuntos laborales relacionados con la Empresa y no podrá ser usado para fines personales, redes sociales, propagación de cadenas, generación de correos masivos ni para realizar ningún acto que contravenga las leyes establecidas en la República de Colombia.
- La infraestructura de servicios de tecnología es limitada y la capacidad de almacenamiento está estandarizada por roles y perfiles, La funcionalidad de los buzones de correo es con el fin de distribución y recepción de información razón por la cual, los usuarios del servicio deben hacer uso adecuado de la capacidad del buzón asignado
- El funcionario o contratista a quien se le asigne buzón de correo electrónico deberá velar por hacer mantenimiento preventivo (eliminar mensajes no necesarios) del buzón y evitar sobrepasar las cuotas asignadas.
- Toda comunicación usando este medio deberá crearse bajo las premisas del respeto y las buenas costumbres, pensando siempre en la buena imagen de la Empresa.

	POLITICA DE SEGURIDAD INFORMATICA	Página 4 de 8
---	--	----------------------

4. SERVICIOS DE RED INALÁMBRICA WIFI

- La red inalámbrica de la compañía deberá estar siempre protegida y separada de la red de PCs, este servicio está restringido solamente a los equipos portátiles y/o dispositivos móviles de la Empresa. Si aplica
- Se autoriza excepcionalmente el uso de este servicio en un segmento de red seguro a equipos y dispositivos móviles de visitantes y/o funcionarios que previamente hayan sido justificados y autorizados por un rol directivo, bajo previa evaluación del Coordinador de Sistemas, para que no se comprometan los intereses de la empresa con riesgos de código malicioso y violación de la normatividad relacionada con los derechos a la propiedad intelectual.
- El portal Cautivo o segmento de red Wifi pública será solo para los usuarios del Terminal de Transportes de Ibagué.

4.1. USO DE SOFTWARE, SISTEMAS DE INFORMACIÓN.

- La adquisición de software, sistemas de información, equipo de cómputo, equipo de red, está sujeta al visto bueno del Coordinador de Sistemas para garantizar la integración con la arquitectura empresarial.
- La instalación y descarga de software en equipo de cómputo de la Empresa está permitido exclusivamente por el Coordinador de Sistemas.
- En los equipos de cómputo de la Empresa, solo se podrá instalar y hacer uso de software licenciado o de uso libre (debidamente justificado por un rol directivo y previamente evaluado por el personal Coordinador de Sistemas para minimizar riesgos de código malicioso y violación de la normatividad relacionada con los derechos a la propiedad intelectual).
- Está prohibido en los equipos de cómputo y dispositivos móviles de la Empresa descargar de internet o desde otra fuente copiar, almacenar, instalar, reproducir canciones, vídeos, películas o cualquier otro tipo de obra o grabación, con excepción a las actividades relacionadas con fines laborales.
- Está prohibido el Uso de equipo de cómputo y/o servicios de internet de la empresa para la copia, reproducción, almacenamiento de material que no cuente con la autorización de uso proporcionada por el propietario de los derechos de autor o por su representante comercial.
- Todo daño causado en los equipos informáticos, así como de los sistemas de información por la intrusión de virus informáticos o programas maliciosos que deriven del software no autorizado, será causal para acciones disciplinarias y/o penales de ser el caso.

4.2. COPIAS DE RESPALDO BACKUPS

- Los usuarios deberán acatar las indicaciones y recomendaciones recibidas por el Coordinador de Sistemas de la Empresa sobre la ubicación, organización de carpetas y archivo de toda información o documento creado

o recibido, mediante medios electrónicos, servicios de red o mediante los aplicativos o sistemas de información usados en la Empresa.

- Las copias de seguridad de las Bases de Datos y de la información consignada en los servidores y su custodia es del Coordinador de Sistemas; se realizará en los medios y plazos establecidos, llevando los respectivos registros.
- Las copias de seguridad de los archivos de usuario ubicados en los equipos de cómputo diferentes a los servidores, son responsabilidad de cada usuario y debe coordinar con el personal de soporte de tecnología la obtención de las copias de respaldo de los mismos.
- La depuración y traslado de la información a los NAS deberá ser solicitada y coordinada por los responsables de cada área con el Coordinador de Sistemas, para que este realice dicho traslado y genere copias de respaldo.
- El Coordinador de Sistemas sólo será responsable del respaldo y continuidad de la información en las carpetas ubicadas y organizadas de acuerdo a las políticas establecidas para copias de respaldo en equipo de cómputo local.

4.3. USO DE EQUIPO DE CÓMPUTO

- El funcionario o contratista es responsable del el uso adecuado del equipo de cómputo y/o dispositivo móvil proporcionado por la Empresa; responsable reportar oportunamente al Coordinador de Sistemas de tecnología las fallas del equipo evidenciadas en la operación del mismo.
- Se procurará la asignación de un único equipo de cómputo para cada usuario, de no ser esto posible, se buscará optimizar los recursos de cómputo con que se cuente.
- Los computadores, dispositivos móviles, correos, internet y demás recursos o servicios de la Empresa no se podrán usar con fines pornográficos o delictivos (terrorismo, soborno, chantaje o cualquier uso que viole leyes de carácter local, nacional o internacional).
- Se deberá apagar adecuadamente el equipo de cómputo y periféricos, una vez que concluya el horario laboral.
- El funcionario o contratista a quien ha sido proporcionado equipo de cómputo portátil y/o dispositivos móviles debe tomar las precauciones necesarias para prevenir el hurto o pérdida del equipo, el acceso no autorizado por terceros a la información almacenada en el equipo fuera de las instalaciones de la Empresa.
- Todo usuario es responsable de conocer el manejo del equipo de cómputo asignado, los sistemas de información y servicios de red que utilizará y de solicitar a quien corresponda la capacitación o entrenamiento en el uso de los mismos.
- La conexión de equipo eléctrico o electrónico será controlada y autorizada formalmente por roles directivos con previa evaluación por el Coordinador de Sistemas y/o personal de Control de instalaciones.
- Las tomas de energía regulada (de color naranja) están restringidas únicamente para la conexión de equipo de cómputo (computadores, monitores).

	POLITICA DE SEGURIDAD INFORMATICA	Página 6 de 8
---	--	----------------------

- El funcionario realizara diariamente higiene al teclado, mouse y pantalla con Alcohol Hiso propílico suministrado por el Coordinador de Sistemas, esto para efectos de autocuidado y protocolo de bioseguridad.

4.4. ACCESO RESTRINGIDO

- La Empresa establecerá áreas físicas y servicios de acceso restringido identificados y delimitados por barreras físicas, lógicas, monitoreados y protegidos con mecanismos de control de acceso que serán registrados y auditados sin previa autorización del usuario o visitante.
- Los roles directivos podrán solicitar y justificar formalmente solicitudes para excepciones a accesos restringidos, las cuales serán evaluadas y autorizadas por el responsable del proceso o del activo correspondiente.
- Está prohibido suministrar información de cualquier tipo de información perteneciente a la configuración de sistemas de información, equipos y servicios de comunicación a terceros fuera de la empresa.

4.5. MANEJO DE INCIDENTES Y CONTROLES DE CAMBIO

- Los responsables de procesos o de activos de información deberán notificar oportuna y formalmente, o mediante un caso al Coordinador de Sistemas, cualquier riesgo o novedad relacionada con la pérdida de confidencialidad, integridad o disponibilidad de información de las bases de datos de la empresa.
- El reemplazo de cualquier componente en sistema de información o recurso de red de la empresa con alta probabilidad de generar incidentes que produzcan pérdida de confidencialidad, disponibilidad e integridad de los datos debe ser gestionado por un plan de cambio.
- El reemplazo de cualquier componente en sistema de información o servicios de red de la empresa con alta probabilidad de generar pérdida de disponibilidad mayor a servicios de red, sistemas de información debe ser gestionado por un plan de cambios.
- Cualquier incidente que involucre perdida de confidencialidad en la información por parte de algún funcionarios será analizado y sancionado por la Gerencia

4.6. CONTINUIDAD DEL NEGOCIO

- De acuerdo con el análisis de impacto en el negocio, de la pérdida de disponibilidad de sistemas de información, servicios de red; Se dispondrán de recursos tecnológicos para la activación de planes de contingencia y recuperación ante desastres para dar continuidad a procesos claves del negocio.
- Los funcionarios deben capacitarse y acatar las instrucciones y acciones a realizar en la activación de planes de contingencia y recuperación ante desastres.

	POLITICA DE SEGURIDAD INFORMATICA	Página 7 de 8
---	--	----------------------

4.7. SANCIONES DISCIPLINARIAS

Quien permita o haga uso inapropiado de sistemas de información, recursos informáticos, accesos restringidos a información o servicios de comunicación de la Empresa, exceda o sobrepase la política de seguridad de la información incurrirá en las sanciones disciplinarias que amerite cada caso, las cuales se aplicaran dependiendo la gravedad de la falta, de su reincidencia de acuerdo con lo establecido en el reglamento interno o documentos que soporten los acuerdos en la relación contractual.

5. DISPOSITIVOS DE ALMACENAMIENTO

Se poseen dos dispositivos NAS D-Link con capacidad de 2 TB, los cuales realizan tareas programadas para el almacenamiento de la información.

Los dispositivos NAS se encuentran ubicados en la oficina de la Coordinación de Sistemas y en la oficina de la Coordinación de la Estación de servicio respectivamente.

6. MÉTODO DE ALMACENAMIENTO.

El método de almacenamiento es incremental, esto quiere decir que todo texto, imagen o archivo se actualiza o se adiciona al Backups anterior.

7. PROCEDIMIENTO COPIA DE SEGURIDAD.

- NAS:
 - **Backups al Servidor Aplicativos (Administrativo - Cafe):** Se realiza la copia 1 vez al día a las 1:00, la cual almacena toda la información, registros, datos de los equipos de cómputo de la entidad y el programa contable Café, se exporta en carpetas, organizadas por dependencia, acompañada de la tarea programada.
 - **Backups al Servidor Gopett (Operativo):** Se realiza la copia de seguridad 3 veces después de cada cierre (7:00 - 15:00 - 23:00) de la base de datos gopett, se exporta a un archivo DMP (Extensión para bases de datos) acompañado de la tarea programada.

Cada dependencia guarda su información, documentos o registros en la carpeta de red asignada, para su debida exportación a los Backups o NAS.

8. ALCANCE DEL ALMACENAMIENTO.

- **Sector Administrativo:** La copia de seguridad, es realizada a toda información, registro o dato que se encuentre ubicado dentro de la carpeta de red.
- **Sector Operativo:** La copia de seguridad, es realizada a la base de datos Gopett.

Elaborado por:

Original Firmada

Henry Alberto Mesa Salcedo
Coordinador de Sistemas

Aprobado por:

Original Firmada

Heber Acosta Bocanegra
Gerente