Política de Seguridad del Hardware e Inventario de Equipos Tecnológicos

TransCaribe
SISTEMA INTEGRADO DE TRANSPORTE MASIVO

Alcaldía Mayor de
Cartagena de Indias

Urb. Anita Diagonal 35 # 71-77
Patio Portal SITM.

Código Postal 130010.

Lunes a viernes
8:00 a.m. a 12:00 p.m. | 1:00 p.m. a 5:00 p.m.

TABLA DE CONTENIDO

1. GENERALIDADES

En TRANSCARIBE S.A., reconocemos que los recursos tecnológicos —como equipos de cómputo, redes, periféricos y dispositivos móviles— son herramientas esenciales para el cumplimiento de nuestra misión institucional y la prestación eficiente del servicio público. Esta política nace con el propósito de establecer una cultura organizacional basada en el uso responsable, el cuidado y la protección de los bienes tecnológicos.

La adecuada gestión del hardware y del inventario tecnológico refleja el compromiso institucional con el uso eficiente, responsable y transparente de los recursos públicos. Esta política fortalece la cultura organizacional orientada a la sostenibilidad, la seguridad de la información y la mejora continua. Asimismo, permite prevenir incidentes operativos y garantizar que los equipos estén disponibles, en óptimas condiciones, para apoyar el desarrollo de las funciones diarias y asegurar la continuidad de los servicios prestados por la entidad.

La política está alineada con los principios de Gobierno Digital, la Política de Seguridad Digital del Estado colombiano y las mejores prácticas internacionales de gestión de activos, como las definidas en la norma ISO/IEC 27002.

2. OBJETIVO

Establecer los lineamientos y responsabilidades que permitan proteger, controlar y gestionar de manera segura y eficiente los equipos tecnológicos de TRANSCARIBE S.A., promoviendo su uso adecuado y su registro actualizado en el inventario institucional. Esta política busca minimizar los riesgos operativos, preservar la integridad de la infraestructura tecnológica y garantizar la disponibilidad de los recursos necesarios para el desarrollo de los procesos de la entidad.

3. ALCANCE

Esta política aplica a todos los procesos de TRANSCARIBE S.A. que hagan uso o gestión de infraestructura tecnológica. Cubre de manera integral todos los activos tecnológicos físicos y lógicos adquiridos por la entidad: servidores, equipos de escritorio, portátiles, dispositivos móviles, equipos de red (como switches, routers, firewalls y puntos de acceso), sistemas de alimentación ininterrumpida (UPS), impresoras, teléfonos IP, máquinas virtuales (VM), instalaciones, personal y cualquier otro componente tecnológico utilizado para el soporte de las operaciones institucionales.

Igualmente, el alcance de esta política se extiende al uso, resguardo, traslado, mantenimiento, control y disposición final de los activos tecnológicos, así como al registro y actualización de los mismos en los sistemas de inventario institucional. Esta política es de obligatorio cumplimiento para todos los servidores públicos que, por razón de sus funciones, accedan, administren o interactúen con los equipos y el software tecnológico propiedad de la entidad.

4. MARCO NORMATIVO

El presente documento se fundamenta en las buenas prácticas empresariales, leyes y normas relacionadas con la seguridad de la información que rigen en Colombia, considerando tanto la protección de datos personales como la gestión integral de la seguridad y continuidad de la información. Entre los principales referentes normativos se destacan:

- Ley 1581 de 2012: Protección de datos personales en Colombia.
- Decreto 1377 de 2013: Reglamenta la Ley 1581.
- Ley 1266 de 2008: Hábeas data financiero, aplicable en ciertos casos específicos.
- Ley 1273 de 2009: Delitos informáticos.
- Decreto 620 de 2020: Política de Seguridad Digital.

- Modelo de Seguridad y Privacidad de la Información (MSPI V.5, mayo de 2025, MinTIC): Guía para la gestión de la seguridad y privacidad de la información en entidades públicas.

- Política de Gobierno Digital: Resolución MinTIC 500 de 2021 y sus actualizaciones.

- Archivo General de la Nación: Ley 594 de 2000 y Decreto 1080 de 2015, en lo relacionado con conservación de documentos electrónicos.

- Normas técnicas internacionales: ISO/IEC 27001:2022 (sistemas de gestión de seguridad de la información), ISO/IEC 27002:2022 (controles de seguridad de la información, literal 5.9 sobre inventario de información y otros activos asociados), y ISO 22301:2019 (gestión de continuidad del negocio).

Este marco normativo sirve como base para la gestión de la seguridad de la información, la protección de los datos personales y la continuidad operativa, asegurando la alineación con los estándares nacionales e internacionales aplicables.

5. RESPONSABLES

Todos los servidores públicos que sean empleados de planta contratados por TRANSCARIBE S.A. son responsables y/o custodios de los activos y bienes tecnológicos entregados para el ejercicio de sus funciones administrativas y operacionales.

En el caso del staff de asesores externos, estos solo podrán ejercer la custodia de los bienes tecnológicos siempre y cuando el responsable del activo lo haya prestado para el desarrollo de tareas y funciones específicas, conforme al objeto de su contratación.

Cabe anotar que ningún asesor externo podrá ser responsable directo de los activos tecnológicos de la entidad.

El Profesional Especializado del Proceso de Gestión en Tecnología, adscrito a la Secretaría General, deberá mantener actualizado el inventario tecnológico del ente gestor.

6. CONDICIONES

Para fortalecer la aplicación y el cumplimiento de las Políticas de Seguridad de la Información, TRANSCARIBE S.A. adoptará las medidas necesarias para garantizar la responsabilidad de todos los servidores públicos, contratistas y terceros que hagan uso de los recursos tecnológicos y de la información institucional.

En ese sentido, toda conducta, acción u omisión que vulnere, incumpla o ponga en riesgo la seguridad de la información o los lineamientos de ciberseguridad definidos por el área de Tecnologías de la Información y las Comunicaciones (TIC) será objeto del procedimiento disciplinario establecido por la entidad, conforme a las disposiciones internas y a la normatividad vigente.

El proceso disciplinario de TRANSCARIBE S.A. será aplicable en todos los casos en los que se evidencie el uso indebido de los sistemas, equipos, redes o información institucional, así como la omisión de los controles y protocolos definidos en las presentes políticas. Dicho proceso garantizará el debido procedimiento, la proporcionalidad de las medidas y la aplicación de las sanciones correspondientes, de acuerdo con la gravedad de la falta cometida.

De esta forma, TRANSCARIBE S.A. reafirma su compromiso con la protección de la información, la gestión responsable de los recursos tecnológicos y el fortalecimiento continuo de la cultura de seguridad y ciberseguridad institucional.

7. EJECUCIÓN

Para ejecutar dicho procedimiento, el Profesional Especializado de la Secretaría General deberá identificar, por dependencias, cómo está distribuida la infraestructura tecnológica, mediante inspección física, con el fin de realizar el levantamiento de esta información. Los datos recolectados

serán registrados en una hoja de Excel, utilizando el formato de hoja de vida de activos tecnológicos.

En el inventario de equipos de escritorio y portátiles se deben registrar los siguientes datos:

- **Tipo de Equipo:** Identificación del equipo en el sistema operativo.

- **Descripción detallada del equipo:** Dentro de este ítem se especificará todos los detalles relevantes de los equipos electrónicos de la entidad.

  - Dirección MAC.
  - Dirección IP (si aplica).
  - Usuario asignado.
  - Estado del equipo.
  - Fecha de asignación.
  - Observaciones técnicas.
  - Responsable y/o custodio del activo.
  - Entre otros.

- **Dependencia:** Se usará la abreviación del nombre de la dependencia, ejemplo: Secretaria General (SG_01) y así sucesivamente.

- **Grupo:** Se especifica dentro de la dependencia al grupo el cual pertenece el equipo.

- **Marca:** Registrar el fabricante del equipo.

- **Proveedor:** A qué empresa se le compro el elemento.

- **Modelo:** Identificar el equipo según el modelo descrito por el fabricante

- **Software:** Se identifican el software instalado.

- **Código del activo:** El código asignado por el módulo de activo fijo del ERP JSP7WEB.

- **Número de Serie:** El número con el que el fabricante identifica sus modelos.

- **Código QR:** Manera en la que se recomienda etiquetar el código del activo asignado por el módulo de activo fijo del ERP JSP7WEB. (Actualmente solo tiene etiquetas numéricas autoadhesivas.).

Todos estos puntos serán la base esencial para crear la hoja de vida de cada uno de los elementos y/o equipos electrónicos que conforman el parque tecnológico de la entidad en su rol administrativo. De igual manera, en esta herramienta se registrarán todas las acciones e incidencias que ocurran respecto a estos activos en el momento en que se hagan efectivas.

El responsable de TI deberá velar por mantener este inventario cien por ciento actualizado al cierre de cada trimestre.

Con el fin de garantizar una gestión eficiente de los recursos tecnológicos, se establecen los siguientes criterios mínimos para declarar equipos como obsoletos:

Antigüedad: Equipos con más de cinco (5) años de uso o que superen la vida útil definida por el fabricante.

Desempeño: Equipos que presenten fallas frecuentes, bajo rendimiento o que no cumplan con los requerimientos mínimos de software actuales.

Compatibilidad: Equipos que no sean compatibles con nuevas versiones de sistemas operativos, aplicaciones corporativas o herramientas de seguridad.

Costos de mantenimiento: Equipos cuyo costo de mantenimiento supere el 50% del valor de un equipo nuevo equivalente.

Seguridad: Equipos que no permitan garantizar la protección de la información o que no cumplan con los estándares de seguridad tecnológica definidos por la entidad.

Estos criterios permiten realizar una gestión planificada y segura de los recursos tecnológicos, optimizando la inversión institucional y asegurando la eficiencia operativa.

8. MATERIALES NECESARIOS

Equipo Computador y portátiles en general.

9. PRODUCTOS ESPERADOS

- Asegurar que los accesos a los sistemas de información y servicios de red de la entidad se realicen de manera controlada y segura.
- Hoja de vida de los equipos que incluye (inventario de incidentes, control sobre los mantenimientos efectuados, cambio y/o reparaciones, estado de los equipos, estado de actualizaciones del software instalados etc.).

10. INDICADORES

- **Tasa de renovación de equipos tecnológicos:** Relación entre el número de equipos adquiridos y el total de equipos reemplazados o dados de baja en el periodo.

  Fórmula: (Equipos adquiridos / Equipos reemplazados o dados de baja) × 100

- **Frecuencia de mantenimiento preventivo y correctivo**: Número total de mantenimientos realizados a los equipos tecnológicos durante el año.

  Fórmula: Total de mantenimientos ejecutados / Año

- **Índice de incidentes técnicos por equipos:** Relación entre el número de incidentes o fallas reportadas y el número total de equipos operativos.

  Fórmula: (Número de incidentes / Total de equipos operativos) × 100

- **Nivel de cumplimiento del mantenimiento preventivo:** Cuántas de las tareas de mantenimiento preventivo planificadas se han realizado efectivamente en un periodo determinado.

  Fórmula: (Mantenimientos ejecutados ÷ Mantenimientos programados) × 100

- **Índice de confiabilidad del inventario:** es un indicador que mide qué tan preciso, actualizado y confiable es el inventario de activos (como equipos, software, licencias, etc.) de una organización.

  Fórmula: (Registros actualizados ÷ Total registros) × 100

11. GLOSARIO:

CPU (Procesador): El "cerebro" de la computadora, que ejecuta instrucciones y procesos.

Tarjeta Madre (Motherboard): El circuito central que conecta todos los componentes internos.

Memoria RAM: Memoria de acceso aleatorio utilizada para la ejecución de aplicaciones y el almacenamiento temporal de datos.

Unidades de almacenamiento (Disco Duro, SSD): Dispositivos para almacenar datos de forma permanente o no volátil.

Fuente de Alimentación: Suministra energía eléctrica a todos los componentes del sistema.

Periféricos: Dispositivos externos conectados a la computadora, como:
Teclado: Dispositivo de entrada para ingresar texto e información.

Ratón (Mouse): Dispositivo apuntador para interactuar con la interfaz gráfica.

Monitor: Dispositivo de salida que muestra la información visual de la computadora.

Impresora: Dispositivo de salida para la impresión de documentos.

Unidad de disco óptico: Un tipo de unidad de disco que utiliza luz láser u ondas electromagnéticas cercanas al espectro de luz como parte del proceso de lectura o escritura de datos hacia o desde discos ópticos**.**

Fuente de alimentación: Una unidad de la computadora que convierte la corriente alterna (CA) de la red eléctrica en CC regulada de bajo voltaje para alimentar todos los componentes de la computadora.

Hardware Básico: Componentes mínimos necesarios para el funcionamiento del equipo, como la CPU y la memoria.

Hardware Complementario: Componentes opcionales que no son necesarios para la funcionalidad básica, pero que añaden capacidades específicas.

Puertos: son los puntos de conexión físicos (hardware) y virtuales (software) que permiten la transferencia de datos, el suministro de energía y la comunicación entre la computadora y otros dispositivos o servicios.

Software: conjunto de programas e instrucciones intangibles que se ejecutan en el hardware.

Usuario: es una persona que utiliza una computadora o un servicio de red.

Rol de usuario: conjunto predefinido de permisos que se asigna a un usuario o grupo de usuarios para controlar qué pueden ver y hacer dentro de un sistema, aplicación o red.

Investigación de rendimiento: Se analizan los componentes de hardware para entender cómo afectan la velocidad y eficiencia de un sistema.

Desarrollo de nuevos productos: Se estudian los componentes físicos para la creación de nuevos dispositivos y tecnologías.

Optimización de sistemas: Se busca la mejora de la interacción entre el hardware y el software para lograr un mejor rendimiento.

12. MARCO DE SEGURIDAD GENERAL:

12.12 SEGURIDAD EN LOS RECURSOS INFORMÁTICOS

Todos los recursos informáticos deben cumplir, como mínimo, con los siguientes criterios de seguridad:

- **Administración de usuarios:** Establece cómo deben ser utilizadas las credenciales de acceso a los recursos informáticos. Define parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiarlas y los períodos de vigencia, entre otros aspectos relacionados con la seguridad de acceso.

- **Rol de usuario:** Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con módulos que permitan definirlos, especificando las acciones permitidas para cada uno. Asimismo, deberán permitir la asignación de diferentes roles a cada usuario, según sus funciones. Los sistemas también deben permitir que ciertos roles tengan privilegios para administrar la gestión de usuarios, garantizando así un control adecuado sobre el acceso y uso de los recursos tecnológicos.

- **Plan de Auditoria:** Corresponde al conjunto de actividades orientadas a la revisión y verificación de las operaciones relacionadas con el funcionamiento y administración de los equipos tecnológicos. Este plan contempla el análisis de las **pistas de auditoría** o registros generados durante la operación de los sistemas, con el fin de garantizar la **trazabilidad, transparencia y control** sobre los procesos técnicos y administrativos.

  La ejecución del plan está a cargo de dos instancias independientes: la **Revisoría Fiscal** y la **Oficina de Control Interno**. Ambas, dentro del marco de sus competencias, realizan auditorías con una periodicidad anual. Estas revisiones permiten identificar posibles desviaciones,

riesgos operativos o debilidades en los controles implementados, y proponer acciones de mejora que fortalezcan la gestión tecnológica y el cumplimiento de las políticas institucionales.

- **Puertas traseras:** Las puertas traseras son accesos no convencionales a los sistemas operativos, bases de datos y aplicativos. Es fundamental reconocer su existencia en la mayoría de estos entornos y llevar a cabo las acciones necesarias para contrarrestar las vulnerabilidades que generan.

- **Control de acceso:** Todos los sistemas de computación del SITM TRANSCARIBE deben contar con mecanismos de acceso mediante códigos de identificación y contraseñas únicas para cada usuario.

- **Contraseñas de acceso:** Las contraseñas utilizadas para acceder a los recursos informáticos, asignadas a servidores públicos, contratistas y otros usuarios, son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgadas bajo ninguna circunstancia.

- **Responsabilidad del usuario:** Los usuarios son responsables de todas las actividades realizadas con su código de identificación y sus contraseñas personales.

- **Identificaciones de usuario:** Se prohíbe el uso de identificaciones de usuario genéricas basadas en funciones laborales. Las identificaciones deben estar asociadas exclusivamente a individuos específicos.

- **Perfiles de usuario:** Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y el cargo de cada persona que accede a él.

- **El Control de súper usuario:** El nivel de súper usuario en los sistemas críticos debe estar sujeto a un control dual, de manera que exista supervisión sobre las actividades realizadas por el administrador del sistema.

- **Protección de la información sensible**: Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe contar con

controles de acceso y estar sometida a procesos de cifrado, con el fin de garantizar que no sea descubierta, modificada, eliminada o inaccesible de manera inapropiada.

- **Seguridad en el desarrollo:** La seguridad debe ser implementada por los diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño, hasta su conversión en un sistema en producción.

- **Separación de ambientes:** Los entornos de desarrollo, pruebas y producción deben mantenerse separados para garantizar una adecuada administración, operación, control y seguridad. En cada uno de ellos se deben instalar las herramientas necesarias para su gestión y funcionamiento.

- **Creación de cuentas de correo institucional:** El Coordinador de Sistemas es responsable de crear las cuentas de correo electrónico institucional para los funcionarios. Estas cuentas deben estar identificadas con la primera letra del primer nombre, el primer apellido completo y, en algunos casos, la primera letra del segundo apellido, o según lo establecido en la política definida para tal fin.

- **Inactivación de correos institucionales:** Los correos electrónicos institucionales serán inactivados conforme a una solicitud formal realizada por la Dirección Administrativa y Financiera.

- **Restricción de acceso en equipos institucionales:** Se restringe el acceso, desde los equipos institucionales, a páginas pornográficas y a todos aquellos sitios cuyo contenido no esté directamente relacionado con el cumplimiento de las actividades laborales.

12.13 DIRECTRICES DE SEGURIDAD INFORMÁTICA PARA LOS SISTEMAS DE LA ENTIDAD.

a) Control de acceso a información privilegiada: Se deben establecer mecanismos para controlar el acceso a información confidencial y privilegiada.

b) Prevención de accesos no autorizados: Es necesario evitar el acceso no autorizado a los sistemas de información, ordenadores y a la información contenida en ellos.

c) Protección de servicios en red: Se deben implementar medidas que garanticen la seguridad de los servicios ofrecidos en red.

d) Detección de actividades no autorizadas: Los sistemas deben contar con herramientas que permitan identificar actividades no autorizadas.

e) Seguridad en dispositivos móviles y teletrabajo: Se debe garantizar la protección de la información cuando se utilicen dispositivos móviles o se trabaje de forma remota.

f) Autorización jerárquica para acceso tecnológico: No se debe permitir el acceso de los usuarios a elementos tecnológicos sin la previa autorización de su superior jerárquico.

g) Baja de usuarios inactivos: Cuando un servidor público deje de ejercer sus funciones, se debe dar de baja su acceso en todos los sistemas de información. Esta solicitud debe ser remitida al responsable de TI por parte de Recursos Humanos, la Dirección Administrativa y Financiera, o el superior jerárquico.

h) Roles y funciones en sistemas de información: Los usuarios y sus roles en los sistemas de información no deben ser segregados en cuanto a sus funciones o tareas, salvo que exista una justificación formal.

12.14 SEGURIDAD PARA USUARIOS TERCEROS AUTORIZADOS

- **Uso de recursos informáticos en equipos externos:** Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de TRANSCARIBE en equipos que no pertenezcan a la entidad, pero que deban ubicarse en sus instalaciones, dichos recursos serán administrados y custodiados por la dependencia solicitante. La configuración inicial será realizada por la Secretaría General, a través del Profesional Especializado, conforme a los lineamientos establecidos.

- **Acceso de terceros a recursos informáticos:** Los terceros contratados por TRANSCARIBE S.A. tendrán acceso únicamente a los recursos informáticos estrictamente necesarios para el cumplimiento de las funciones para las cuales fueron vinculados. Dichos accesos deberán ser aprobados por su jefe inmediato.

  Además, el responsable del recurso entregado deberá asumir la custodia del activo informático y firmar el acta de entrega correspondiente, garantizando así el control y la trazabilidad del uso de los recursos tecnológicos.

- **Conexión entre sistemas internos y externos:** Toda solicitud de conexión entre los sistemas internos de la entidad y sistemas de terceros debe ser gestionada por el jefe inmediato correspondiente. La aprobación e implementación de dicha conexión estará a cargo del Profesional Especializado del área de Secretaría General, con el fin de garantizar que no se comprometa la seguridad de la información de la entidad.

- **Interconexión de redes con terceros:** Como requisito para interconectar las redes de TRANSCARIBE S.A. con las de terceros, los sistemas de comunicación externos deben cumplir con los estándares y requisitos técnicos establecidos por la entidad. TRANSCARIBE S.A. se reserva el derecho de monitorear dichos sistemas sin previo aviso, con el fin de evaluar su nivel de seguridad.

  Asimismo, la entidad podrá cancelar o terminar cualquier conexión con sistemas de terceros que no cumplan con los requerimientos internos definidos. Toda comunicación entre TRANSCARIBE y el tercero será monitoreada, tanto en sentido de envío como de recepción, para garantizar la integridad y seguridad de la información institucional.

- **Registro y gestión de equipos electrónicos:** La mesa de ayuda, en cada proceso de soporte técnico, deberá recolectar toda la información relevante de los equipos electrónicos, incluyendo número de serie, modelo, propietario o responsable, entre otros datos. Esta información permitirá gestionar e implementar una herramienta dinámica que facilite la consulta mediante métodos como códigos de barras o códigos internos asignados a cada activo.

- **Control de ingreso y salida de equipos electrónicos:** Cada elemento electrónico debe contar con un registro de ingreso y/o salida, estos elementos no pueden salir del edificio administrativo si previa autorización de jefe jerárquico, visto del responsable de TI y visto bueno del responsable de almacén si el equipo es propio de la entidad.

- **Contratos con terceros y seguridad de la información:** Toda relación contractual con proveedores, contratistas o terceros que presten servicios de soporte, mantenimiento o gestión de equipos tecnológicos deberá incluir:

  1) Acuerdos de confidencialidad (NDA) que protejan la información sensible de la entidad.

  2) Acuerdos de nivel de servicio (SLA) que definan compromisos, condiciones de atención, tiempos de respuesta y niveles de disponibilidad requeridos.

  3) Cláusulas de seguridad de la información, orientadas a proteger los activos tecnológicos, prevenir el acceso o divulgación no autorizada y garantizar el cumplimiento de las políticas institucionales de tecnología y seguridad.

  Desde TI, en coordinación con las dependencias competentes, velaran por el cumplimiento de estos acuerdos y su adecuada incorporación en los procesos contractuales que el ente gestor firme con terceros.

12.15 POLÍTICA DE SOFTWARE UTILIZADO

- Todo el software utilizado por TRANSCARIBE será adquirido conforme a las normas vigentes, siguiendo los procedimientos específicos de la entidad y sus reglamentos internos.

- Todo el software de manejo de datos utilizado por TRANSCARIBE dentro de su infraestructura informática deberá incorporar las técnicas más

avanzadas de la industria, con el fin de garantizar la integridad de los datos.

- TRANSCARIBE deberá contar con un inventario actualizado de las licencias de software, que permita su adecuada administración y control, evitando posibles sanciones por la instalación de software no licenciado.

- El Profesional Especializado de la Secretaría General realizará revisiones periódicas a los computadores de escritorio, tabletas y portátiles asignados a los servidores públicos de TRANSCARIBE S.A., con el fin de monitorear la presencia de software malicioso (como virus, malware o spyware) y verificar que no se encuentren instalados programas que puedan comprometer la seguridad de la red institucional, afectar la integridad de la información o infringir las normas de derecho de autor.

  Estas revisiones se complementarán con controles técnicos centralizados desde el servidor de dominio, orientados a la administración de políticas de seguridad, autenticación y restricciones para la instalación o ejecución de software no autorizado.

- TRANSCARIBE promoverá el uso de herramientas de Prevención de Pérdida de Datos (DLP) y Gestión de Dispositivos Móviles (MDM), con el propósito de fortalecer la protección de los equipos portátiles y móviles corporativos, prevenir fugas de información y garantizar el cumplimiento de las políticas institucionales de seguridad de la información y uso aceptable de los recursos tecnológicos.

- Si la entidad cuenta con la capacidad para adquirir herramientas de Prevención de Pérdida de Datos (DLP – Data Loss Prevention), se recomienda que su adquisición sea gestionada desde Tecnología de la Información (TI), con el fin de asegurar el monitoreo, bloqueo, transferencia o uso no autorizado de datos sensibles o confidenciales dentro de la organización.

12.16 POLÍTICA DE ACTUALIZACIÓN DE HARDWARE

- Cualquier modificación que se requiera realizar en los computadores de escritorio, tabletas, portátiles o servidores de TRANSCARIBE S.A. (como cambios de procesador, adición de memoria, disco duro o tarjetas) deberá contar previamente con una evaluación técnica y la autorización del Profesional Especializado de la Secretaría General.

- La reparación técnica de los equipos que implique su apertura solo podrá ser realizada por personal debidamente autorizado.

- Los equipos de microcomputación (PC, servidores, LAN, etc.) no deben ser movidos ni reubicados sin la aprobación previa del Profesional Especializado de la Secretaría General.

13. CONTROL DE CAMBIOS

FECHA	DESCRICPCION DE CAMBIOS	VERSION
2025/06/13	Versión definitiva, recopilación de las versiones anteriores proyectadas.	1.0

14. VALIDACIÓN DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: Gerardo Marriaga Tovar. **Cargo:** Profesional Especializado. **Fecha:** 13-06-2025	**Nombre:** Marcela Chedrauy Araujo. **Cargo:** Secretaria General. **Fecha:** 30-06-2025	**Nombre:** Comité de Gestión y Desempeño **Fecha:** 06-11-2025