

RESOLUCIÓN No. 351 DE 2026
(24 SEP 2026)

POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA INSTITUCIONAL PARA EL BUEN USO DE TECNOLOGÍAS INFORMÁTICAS DE LA E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA Y SE DICTAN OTRAS DISPOSICIONES

EL GERENTE DE LA E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA,

En uso de sus atribuciones constitucionales, legales y,

CONSIDERANDO

Que la Constitución Política de Colombia establece la obligación de las entidades públicas de proteger la información de las personas y garantizar el adecuado cumplimiento de las funciones administrativas y misionales.

Que la Ley 87 de 1993 establece normas para el ejercicio del control interno en las entidades y organismos del Estado, orientadas a garantizar la protección de los recursos, la eficacia de las operaciones y la adecuada administración de la información.

Que la Ley 594 de 2000 establece disposiciones relacionadas con la gestión y conservación de los documentos y archivos públicos.

Que la Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales, aspecto de especial relevancia para una institución hospitalaria que realiza tratamiento de información personal y datos sensibles.

Que el Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, establece disposiciones relacionadas con el sector TIC y la Política de Gobierno Digital.

Que el Modelo Integrado de Planeación y Gestión – MIPG establece la seguridad de la información y la adecuada gestión de los recursos tecnológicos como elementos necesarios para fortalecer la gestión institucional y la generación de valor público.

Que mediante la Resolución 500 de 2021, el Ministerio de Tecnologías de la Información y las Comunicaciones estableció lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, así como lineamientos para la gestión de riesgos de seguridad de la información y seguridad digital.

Que mediante la Resolución 2277 de 2025, el Ministerio de Tecnologías de la Información y las Comunicaciones actualizó el Modelo de Seguridad y Privacidad de la Información, fortaleciendo su alineación con la norma ISO/IEC 27001:2022.

Que el Modelo de Seguridad y Privacidad de la Información contempla la necesidad de establecer políticas, responsabilidades, controles y procedimientos para garantizar el adecuado uso y protección de los activos de información de las entidades públicas.

Que la norma ISO/IEC 27001:2022 establece un marco para la gestión de los riesgos relacionados con la seguridad de la información y contempla controles asociados con la gestión y protección de los activos tecnológicos, seguridad de los dispositivos de usuario final, gestión de accesos, protección contra software malicioso, respaldo de información y reporte de eventos de seguridad.

Que la E.S.E. Hospital Universitario San Rafael de Tunja dispone de equipos de cómputo, dispositivos móviles, servidores, sistemas de información, redes, medios de almacenamiento, herramientas de comunicación y demás recursos tecnológicos necesarios para el desarrollo de sus actividades asistenciales, administrativas, financieras, académicas y de apoyo.

Que el uso inadecuado de los recursos tecnológicos puede generar riesgos de pérdida, alteración, divulgación, indisponibilidad o acceso no autorizado a información institucional y, particularmente, a información clínica y datos personales de pacientes, usuarios, colaboradores y terceros.

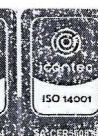
Que resulta necesario establecer reglas institucionales claras para el uso responsable, seguro, eficiente y adecuado de los equipos y herramientas informáticas, así como determinar las responsabilidades de los usuarios y del área responsable de Tecnología de la Información.

Justificación

La E.S.E. Hospital Universitario San Rafael de Tunja reconoce la importancia de garantizar el uso adecuado, seguro, eficiente y responsable de los equipos y herramientas informáticas institucionales, como elementos fundamentales para el desarrollo de sus actividades misionales, asistenciales, administrativas, docentes e investigativas.

Por este motivo, se hace necesario adoptar la Política Institucional para el Buen Uso de Equipos y Herramientas Informáticas, con el propósito de establecer lineamientos y responsabilidades que permitan proteger los recursos tecnológicos, fortalecer la seguridad y privacidad de la información, prevenir riesgos asociados al uso inadecuado y promover la continuidad y eficiencia de los servicios institucionales.

La presente política contribuye al cumplimiento de los objetivos institucionales, el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y la consolidación de una cultura de uso responsable y seguro de la tecnología por parte de todos los usuarios autorizados



RESUELVE

ARTÍCULO 1. ADOPCIÓN: Adoptar la Política Institucional para el Buen Uso De Tecnologías Informáticas de la E.S.E. Hospital Universitario San Rafael de Tunja, como instrumento institucional orientado a establecer los principios, lineamientos, responsabilidades y reglas para el uso adecuado, seguro, eficiente y responsable de los recursos tecnológicos puestos a disposición de funcionarios, trabajadores, contratistas, practicantes, estudiantes, proveedores y terceros autorizados.

"La E.S.E. Hospital Universitario San Rafael de Tunja se compromete a garantizar el uso adecuado, seguro, eficiente, responsable y racional de los equipos, sistemas, herramientas y demás recursos informáticos y tecnológicos institucionales, promoviendo su utilización exclusivamente para el cumplimiento de las funciones, actividades y objetivos institucionales, y protegiendo la información frente a accesos, usos, divulgaciones, modificaciones, pérdidas o afectaciones no autorizadas."

ARTÍCULO 2. OBJETIVO GENERAL: Establecer los lineamientos para el Buen Uso De Tecnologías Informáticas institucionales, con el propósito de proteger la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información, garantizar la continuidad de los servicios y reducir los riesgos asociados al uso de los recursos tecnológicos.

ARTÍCULO 3. ALCANCE: La presente política aplica a todos los funcionarios independientemente de su modalidad de vinculación, y se extiende de manera obligatoria a funcionarios, contratistas, proveedores, personal en formación y en desarrollo de prácticas académicas, usuarios externos autorizados y demás terceros que tengan acceso a equipos, sistemas, redes de datos, aplicaciones, servicios tecnológicos o información de la E.S.E. Hospital Universitario San Rafael de Tunja.

Responsabilidades: La implementación y desarrollo de la política institucional para el buen uso de equipos y herramientas informáticas, estará bajo la responsabilidad del Subproceso de Tecnologías de la Información, a través del equipo de Seguridad de la Información, el cual será el encargado de liderar su ejecución, seguimiento, monitoreo y mejora continua, en articulación con los procesos institucionales.

Los coordinadores y líderes de proceso apoyarán en su implementación, al igual, que los colaboradores en cumplimiento de sus funciones.

Mecanismos De Implementación: La implementación, desarrollo, seguimiento y cumplimiento de la política institucional para el buen uso de uso inadecuado de tecnologías

informáticas, se realizará a través de los lineamientos definidos en los procedimientos S-PR-45 Identificación De Uso Inadecuado De Tecnologías Informáticas y A-PR-17 Gestión por pérdida, robo, hurto, o siniestro de activos fijos, los cuales hacen parte integral de la presente resolución.

ARTÍCULO 4. USO DE LOS EQUIPOS INFORMÁTICOS: Los equipos asignados por la E.S.E. deberán ser utilizados de manera responsable y exclusivamente por el usuario autorizado.

Los usuarios deberán:

1. Utilizar el equipo asignado para el desarrollo de sus funciones o actividades autorizadas.
2. Mantener el equipo en condiciones adecuadas de operación.
3. Evitar golpes, manipulación indebida, exposición a líquidos, alimentos, temperaturas extremas o condiciones que puedan deteriorarlo.
4. Bloquear la sesión cuando se ausenten temporalmente del puesto de trabajo.
5. Apagar o cerrar adecuadamente el equipo cuando las condiciones de operación lo permitan.
6. Reportar oportunamente cualquier falla, daño, pérdida o comportamiento inusual.
7. Permitir las actividades de mantenimiento, actualización, revisión o soporte autorizadas por el subproceso de Tecnologías de la Información.
8. Mantener actualizado el sistema operativo y las aplicaciones conforme a los mecanismos establecidos por Tecnología.
9. Utilizar únicamente software autorizado.
10. Proteger los equipos portátiles y dispositivos móviles durante su traslado y utilización fuera de las instalaciones.
11. Toda solicitud de servicios técnicos deberá ser tramitada a través de la mesa de servicios.

ARTÍCULO 5. PROHIBICIONES: Queda prohibido:

1. Prestar equipos institucionales a personas no autorizadas.
2. Instalar software sin autorización del subproceso de Tecnologías de la Información.
3. Deshabilitar antivirus, mecanismos de seguridad, actualizaciones o controles institucionales.
4. Modificar configuraciones de seguridad sin autorización.
5. Conectar dispositivos externos no autorizados.
6. Utilizar los equipos para actividades ilícitas.
7. Utilizar programas, aplicaciones o servicios que puedan comprometer la seguridad institucional.
8. Intentar acceder a información, sistemas o cuentas para los cuales no se tengan permisos.
9. Alterar, eliminar o manipular registros, archivos o configuraciones sin autorización.
10. Utilizar las credenciales de otra persona.



11. Facilitar las credenciales institucionales a terceros.
12. Almacenar información institucional en servicios personales no autorizados.
13. Descargar o instalar contenido que represente un riesgo para la infraestructura tecnológica.
14. Utilizar los recursos tecnológicos institucionales para actividades que puedan afectar la imagen, seguridad o reputación de la E.S.E.

ARTÍCULO 6. SOFTWARE Y APLICACIONES: Todo software instalado en los equipos institucionales deberá contar con autorización del subproceso de Tecnologías de la Información y cumplir con las condiciones legales de licenciamiento.

El usuario no podrá instalar programas por iniciativa propia cuando estos puedan representar riesgos de seguridad, afectar el funcionamiento del equipo o generar incumplimiento de las condiciones de licenciamiento.

Tecnologías de la Información podrá retirar aplicaciones no autorizadas que representen riesgos para la infraestructura institucional.

ARTÍCULO 7. CORREO ELECTRÓNICO INSTITUCIONAL: El correo electrónico institucional constituye una herramienta de trabajo y deberá utilizarse principalmente para actividades relacionadas con las funciones institucionales. Los usuarios deberán:

1. Proteger sus credenciales.
2. Evitar compartir contraseñas.
3. Verificar el remitente de mensajes sospechosos.
4. No abrir archivos o enlaces sospechosos.
5. Reportar inmediatamente mensajes que puedan corresponder a phishing, malware o fraude.
6. Evitar el envío de información institucional a cuentas personales, salvo autorización.
7. Verificar los destinatarios antes de enviar información sensible.
8. Aplicar especial cuidado cuando el mensaje contenga información clínica, datos personales o información reservada.
9. Adherirse a los controles de seguridad definidos por la institución, ejemplo: doble factor de autenticación.
10. Depurar bandejas de entrada, salida, que no se requieran.

ARTÍCULO 8. CONTRASEÑAS Y CREDENCIALES: Las credenciales de acceso son personales e intransferibles. Cada usuario deberá:

- Mantener la confidencialidad de sus contraseñas.
- No compartirlas con compañeros, contratistas o terceros.



- Utilizar mecanismos de autenticación establecidos por el subproceso de Tecnologías de la Información.
- Cambiar las credenciales cuando exista sospecha de compromiso.
- Reportar inmediatamente la pérdida o exposición de una credencial.
- Evitar almacenar contraseñas en medios no autorizados.

El personal de soporte tecnológico no deberá solicitar al usuario que revele su contraseña, salvo mecanismos institucionales excepcionalmente definidos para administración técnica y bajo controles autorizados.

ARTÍCULO 9. PROTECCIÓN DE LA INFORMACIÓN CLÍNICA: Por tratarse de una institución hospitalaria, todo usuario que tenga acceso a historias clínicas, información de pacientes, resultados diagnósticos, imágenes, información administrativa o cualquier otro dato sensible deberá observar estrictamente los principios de confidencialidad, seguridad y acceso autorizado.

El acceso a la información clínica deberá limitarse a lo estrictamente necesario para el cumplimiento de las funciones asignadas.

Queda prohibido consultar y/o compartir información de pacientes por razones personales, familiares, curiosidad, interés particular o cualquier finalidad diferente a la autorizada institucionalmente.

ARTÍCULO 10. MEDIOS REMOVIBLES: El uso de discos externos y otros medios removibles deberá estar controlado de acuerdo con los lineamientos establecidos por Tecnologías de la Información. Cuando su utilización sea necesaria, deberá garantizarse que:

- El dispositivo sea autorizado.
- Se realicen controles de seguridad, (encriptamiento)
- Se evite la transferencia innecesaria de información.
- La información sensible sea protegida.
- Se eliminen los archivos cuando ya no sean necesarios, conforme a las políticas de gestión de información.

ARTÍCULO 11. EQUIPOS PORTÁTILES Y DISPOSITIVOS MÓVILES: Los equipos portátiles y dispositivos móviles institucionales deberán contar con los mecanismos de protección definidos por Tecnologías de la Información.

Cuando sean utilizados fuera de las instalaciones de la E.S.E., el usuario deberá adoptar medidas razonables para evitar pérdida, hurto, acceso no autorizado o exposición de la información.



La pérdida o extravío de un equipo deberá ser reportada inmediatamente a los subprocesos de Tecnologías de la Información y Gestión de Suministros y Activos Fijos y al jefe inmediato.

ARTÍCULO 12. ACCESO A INTERNET: El acceso a Internet desde la infraestructura institucional deberá realizarse de forma responsable y de acuerdo con las necesidades propias de las funciones institucionales.

La E.S.E. podrá implementar mecanismos de filtrado, monitoreo, bloqueo y control del tráfico de red para prevenir riesgos de seguridad, malware, fuga de información y uso indebido de los recursos tecnológicos, dentro del marco legal aplicable.

ARTÍCULO 13. MONITOREO Y REGISTRO: La E.S.E., a través del subproceso responsable de Tecnologías de la Información y Seguridad de la Información, podrá implementar mecanismos técnicos de monitoreo, registro y auditoría sobre los recursos tecnológicos institucionales, con el propósito de:

- Proteger los activos de información.
- Detectar incidentes de seguridad.
- Investigar eventos.
- Identificar vulnerabilidades.
- Garantizar la disponibilidad de los servicios.
- Cumplir requisitos legales y de auditoría.
- Fortalecer la seguridad institucional.

El monitoreo deberá realizarse conforme a las políticas de privacidad y protección de datos personales y los principios de necesidad, proporcionalidad y finalidad.

ARTÍCULO 14. MANTENIMIENTO DE EQUIPOS: El mantenimiento preventivo y correctivo de los equipos institucionales deberá ser realizado por personal autorizado o proveedores contratados por la E.S.E.

El mantenimiento de los equipos de servicios tercerizados, será responsabilidad exclusiva de los mismos, adhiriéndose a los controles y políticas institucionales.

Los usuarios no deberán realizar reparaciones, modificaciones de hardware o intervenciones técnicas no autorizadas.

Toda intervención deberá procurar preservar la información almacenada y mantener la trazabilidad correspondiente.



ARTÍCULO 15. TRASLADO, PRÉSTAMO Y RETIRO DE EQUIPOS: Ningún equipo, dispositivo, medio de almacenamiento o activo tecnológico institucional podrá ser retirado de las instalaciones sin la autorización correspondiente.

Los traslados, préstamos o reasignaciones deberán quedar registrados de acuerdo con los procedimientos institucionales de administración de activos.

La gestión de activos tecnológicos deberá contemplar mecanismos para prevenir pérdida, daño, robo, acceso no autorizado y afectación de la operación, en concordancia con los lineamientos del MSPI.

ARTÍCULO 16. REPORTE DE INCIDENTES: Todo usuario deberá reportar inmediatamente al subproceso de Tecnologías de la Información cualquier situación que pueda afectar la seguridad de los equipos o de la información, incluyendo:

- Pérdida o hurto de equipos.
- Acceso no autorizado.
- Malware o virus.
- Correos sospechosos.
- Phishing.
- Divulgación accidental de información.
- Pérdida de información.
- Alteración de archivos.
- Fallas de seguridad.
- Uso indebido de cuentas.
- Instalación no autorizada de software.
- Comportamientos anormales de los sistemas.

El reporte deberá realizarse mediante los canales institucionales definidos, para la gestión de incidentes de seguridad de la información.

ARTÍCULO 17. RESPONSABILIDADES DE LOS USUARIOS: Son responsabilidades de los usuarios:

1. Conocer y cumplir esta política.
2. Proteger los equipos y herramientas asignados.
3. Proteger las credenciales de acceso.
4. Utilizar adecuadamente los recursos tecnológicos.
5. Mantener la confidencialidad de la información.
6. Reportar incidentes oportunamente.
7. Participar en las capacitaciones de seguridad de la información.
8. Cumplir las políticas y procedimientos relacionados con seguridad y privacidad de la información.



9. Devolver los equipos y activos tecnológicos cuando finalice la relación laboral, contractual, académica o de prestación del servicio.
10. Abstenerse de realizar actividades que puedan comprometer la seguridad de la infraestructura tecnológica.

ARTÍCULO 18. RESPONSABILIDADES DEL SUBPROCESO DE TECNOLOGÍAS DE LA INFORMACIÓN: El subproceso es responsable de:

1. Administrar los recursos tecnológicos institucionales.
2. Establecer controles técnicos de seguridad.
3. Gestionar las vulnerabilidades de los equipos.
4. Mantener mecanismos de protección contra software malicioso.
5. Gestionar actualizaciones y parches de seguridad.
6. Administrar los accesos tecnológicos.
7. Gestionar los incidentes tecnológicos y de seguridad de la información.
8. Mantener actualizado el inventario de activos tecnológicos.
9. Realizar mantenimiento preventivo y correctivo.
10. Implementar mecanismos de respaldo y recuperación de información conforme a las políticas institucionales.
11. Promover campañas de capacitación y sensibilización.
12. Realizar seguimiento al cumplimiento de esta política.
13. Proponer las actualizaciones que sean necesarias.

ARTÍCULO 19. RESPONSABILIDADES DE LOS JEFES Y LÍDERES DE PROCESO Y SUPERVISORES: Los coordinadores, líderes de proceso y supervisores deberán:

1. Garantizar que los usuarios bajo su responsabilidad utilicen adecuadamente los recursos tecnológicos.
2. Informar oportunamente los cambios de personal que impliquen creación, modificación o retiro de accesos.
3. Solicitar los recursos tecnológicos requeridos de acuerdo con las necesidades del proceso.
4. Reportar daños, pérdidas o usos indebidos.
5. Promover el cumplimiento de esta política.
6. Participar en la identificación y actualización y gestión de los activos de activos de información.
7. Participar en la identificación y gestión de los riesgos de seguridad de la información relacionados con sus procesos.

ARTÍCULO 20. RESPONSABILIDADES DE CONTRATISTAS, PERSONAL EN FORMACIÓN, PRACTICANTES, PROVEEDORES Y TERCEROS: Los contratistas, personal en formación practicantes, proveedores y demás terceros que tengan acceso a recursos



tecnológicos institucionales deberán cumplir esta política y las demás disposiciones de seguridad de la información aplicables.

El acceso estará limitado a los recursos estrictamente necesarios para el cumplimiento de las actividades autorizadas.

ARTÍCULO 21. CAPACITACIÓN Y SENSIBILIZACIÓN: La E.S.E., a través del subproceso de Tecnologías de la Información y/o Seguridad de la Información, en coordinación con Gestión de Talento Humano mediante el plan de formación institucional, desarrollará actividades periódicas de sensibilización sobre:

- Buen uso de equipos.
- Seguridad de la información. (Políticas y Controles)
- Protección de datos personales.
- Contraseñas.
- Phishing.
- Malware.
- Ingeniería social.
- Manejo seguro del correo electrónico.
- Protección de información clínica.
- Reporte de incidentes.
- Uso seguro de dispositivos móviles.
- Responsabilidades de los usuarios.

ARTÍCULO 22. EXCEPCIONES: Las excepciones a esta política deberán estar debidamente justificadas, documentadas y autorizadas por la instancia competente de acuerdo con el procedimiento institucional de gestión de excepciones de seguridad de la información.

Las excepciones deberán considerar los riesgos asociados y, cuando corresponda, establecer controles compensatorios.

ARTÍCULO 23. REVISIÓN Y ACTUALIZACIÓN: La presente política será revisada como mínimo una vez al año o cuando se presenten cambios normativos, tecnológicos, organizacionales, riesgos significativos, incidentes de seguridad o modificaciones en los procesos institucionales que hagan necesaria su actualización.

La revisión estará a cargo del subproceso de Tecnologías de la Información, con participación de los procesos y subprocesos que correspondan.



ARTÍCULO 24. DIVULGACIÓN: La presente política deberá ser divulgada a todos los funcionarios, trabajadores, contratistas, estudiantes, practicantes, proveedores y terceros que tengan acceso a los recursos tecnológicos institucionales.

La política deberá mantenerse disponible a través de los medios institucionales definidos para la publicación de documentos del Sistema Integrado de Gestión.

ARTICULO 25. SEGUIMIENTO Y EVALUACIÓN:

El seguimiento a su ejecución se realizará a través del Comité Institucional de Gestión y Desempeño, en el marco de sus funciones y responsabilidades y a través del siguiente indicador:

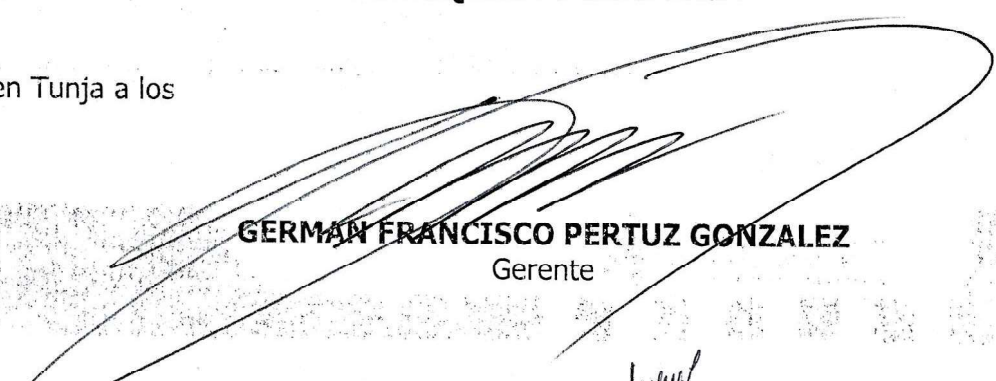
2910 Porcentaje de daño de equipos de Tecnología Informática atribuible al uso inadecuado

Aplicación de lista de chequeo S-F-79 Lista De Chequeo Seguimiento Controles ISO 27001-2022 y Rondas de seguridad.

ARTÍCULO 26. VIGENCIA: La presente Resolución rige a partir de la fecha de su expedición y publicación y será de obligatorio cumplimiento para las personas comprendidas dentro de su ámbito de aplicación.

PUBLIQUESE Y CUMPLASE

Dada en Tunja a los


GERMAN FRANCISCO PERTUZ GONZALEZ
Gerente

Revisó: Marbíz Said Ducuara Amado/ Profesional Universitario TI 

Revisó: Javier Andres Gallo Ocampo/ Asesor Desarrollo de Servicios 

Revisó: Diana Carolina Uribe Rodríguez/ Coordinadora de Gestión de Calidad 

Revisó: Julián Camilo Niño/ Asesor Jurídico Gerencia. 

Proyectó: Jorge Armando Figueredo Malagón /Profesional Especializado 