TABLA DE CONTENIDO

COPIA CONTROLADA

COPIA CONTROLADA

COPIA CONTROLADA

COPIA CONTROLADA

COPIA CONTROLADA

INTRODUCCIÓN

La base para que una organización opere de manera confiable en materia de seguridad informática es la definición de políticas y estándares adecuados que permitan minimizar los riesgos. Actualmente, es imposible hablar de un sistema completamente seguro, ya que el costo de alcanzar una protección total resultaría excesivo.

Las políticas de seguridad de la información constituyen el plan de acción de una empresa para gestionar los riesgos asociados a la protección de sus activos informáticos. Surgen como una herramienta organizacional destinada a concienciar a todos los miembros de la compañía sobre la importancia, sensibilidad y correcto manejo de la información.

La creación de una política corporativa sólida permite a la empresa desarrollarse y mantenerse competitiva en su sector. Dicha política debe ser elaborada y aprobada por la alta dirección, e involucrar el compromiso de todas las áreas de la organización, dado que la seguridad es una responsabilidad colectiva.

No obstante, homogeneizar los criterios de seguridad representa una tarea compleja, especialmente cuando la empresa cuenta con distintas áreas que requieren enfoques específicos. Por ello, es fundamental que las políticas de seguridad sean de conocimiento general y se apliquen de manera coherente en toda la organización.

COPIA CONTROLADA

La seguridad informática es una función estratégica que implica evaluar, mitigar y administrar los riesgos tecnológicos, con base en políticas y estándares que respondan a las necesidades de la Red de Salud del Centro en materia de protección de la información y continuidad operativa.

1. OBJETIVO

Establecer, documentar y difundir las políticas y estándares de seguridad informática en la Red de Salud del Centro, con el fin de garantizar su conocimiento, comprensión y cumplimiento obligatorio por parte de todo el personal en el uso adecuado de los recursos informáticos asignados, en busca de asegurar la integridad, disponibilidad y confidencialidad de la información institucional mediante la aplicación de disposiciones que regulen el acceso, manejo y protección de los sistemas y datos bajo responsabilidad del personal.

1.1. OBJETIVOS ESPECÍFICOS

- Proteger al personal y reducir riesgos mediante la aplicación de lineamientos y controles obligatorios que minimicen la exposición a riesgos operativos, tecnológicos y de información, en cumplimiento de normas institucionales y regulaciones aplicables.

COPIA CONTROLADA

- Implementar y mantener medidas de seguridad física y ambiental que salvaguarden instalaciones, infraestructura, servicios críticos y activos de información, conforme a los estándares institucionales.
- Estandarizar la administración y operación de equipos de cómputo, asegurando su inventario, configuración adecuada, uso autorizado, mantenimiento preventivo y protección frente a amenazas internas y externas.
- Aplicar mecanismos de control de acceso lógico (autenticación, autorización y monitoreo) que garanticen el uso exclusivo de sistemas, redes y recursos por personal autorizado, asegurando trazabilidad y cumplimiento de políticas.
- Asegurar el cumplimiento continuo de políticas y normativas internas y externas en materia de seguridad informática, promoviendo la adopción de buenas prácticas en la gestión de la información.
- Definir y regular lineamientos de seguridad para teletrabajo, garantizando la confidencialidad, integridad y disponibilidad de la información procesada o almacenada fuera de las instalaciones físicas.

COPIA CONTROLADA

2. ALCANCE

El presente manual aplica a todo el personal de la Red de Salud del Centro y abarca los lineamientos y controles relacionados con la seguridad del personal, la seguridad física y ambiental, la administración y protección de equipos de cómputo, los controles de acceso lógico, el cumplimiento normativo en materia de seguridad informática y las medidas de

protección asociadas al teletrabajo, garantizando la correcta gestión y protección de la información institucional en todas las actividades operativas y administrativas.

3. DEFINICIONES

Acceso físico: Actividad que consiste en ingresar a un área o instalación específica.

Acceso lógico: Capacidad de comunicarse y conectarse a un activo tecnológico para su utilización.

Acceso remoto: Conexión entre dos dispositivos de cómputo ubicados en distintos lugares físicos mediante líneas de comunicación, ya sean telefónicas o redes de área amplia (WAN), que permiten el acceso a aplicaciones e información de la red. Este tipo de acceso suele requerir un sistema robusto de autenticación.

Antivirus: Programa informático diseñado para detectar, bloquear y eliminar virus u otros tipos de código malicioso presentes en discos duros u otros medios electrónicos de almacenamiento.

Ataque: Conjunto de acciones orientadas a vulnerar las medidas de protección de un activo, con el fin de obtener acceso no autorizado o causar daño.

COPIA CONTROLADA

Base de datos: Conjunto estructurado de datos relacionados, almacenados y gestionados para satisfacer los requerimientos de procesamiento y recuperación de información de una organización o individuo.

Confidencialidad: Principio de seguridad que implica la obligación de no divulgar información a personas no autorizadas para su conocimiento o uso.

Contraseña: Secuencia de caracteres utilizada para autenticar la identidad de un usuario y permitir su acceso a un sistema, aplicación o red.

Control de acceso: Mecanismo de seguridad que previene y detecta accesos no autorizados, permitiendo únicamente el acceso legítimo a los activos tecnológicos.

Copyright: Derecho del autor sobre sus obras, incluidos los programas informáticos, que le permite decidir en qué condiciones pueden ser reproducidas o distribuidas. Aunque este derecho es irrenunciable, su ejercicio puede ser tan restrictivo o amplio como el autor determine.

Disponibilidad: Condición que garantiza que la información y los servicios estén accesibles y utilizables en el momento en que se necesiten.

Estándar: Conjunto de reglas, procedimientos o lineamientos obligatorios que proporcionan estructura y dirección a las políticas, garantizando su efectividad.

COPIA CONTROLADA

Falta administrativa: Acción u omisión contraria a la normatividad vigente, cometida por un servidor público, que genera responsabilidad y sanción conforme a la ley.

FTP (File Transfer Protocol): Protocolo estándar de comunicación que permite la transferencia de archivos entre computadoras a través de una red.

Gusano: Programa informático capaz de replicarse y propagarse automáticamente a otros sistemas mediante redes, causando saturación o afectación de recursos.

Hardware: Conjunto de componentes físicos y características técnicas que conforman una computadora o dispositivo electrónico.

Herramientas de seguridad: Mecanismos automatizados que protegen la infraestructura tecnológica de una organización frente a amenazas o vulnerabilidades.

Identificador de usuario (User ID): Nombre único asignado a un usuario para acceder a los sistemas y equipos institucionales, permitiendo su identificación y registro de actividades.

Impacto: Magnitud del daño potencial o real que puede sufrir un activo si una amenaza se materializa.

Incidente de seguridad: Cualquier evento que ponga en riesgo la confidencialidad, integridad o disponibilidad de la información o los sistemas de la organización.

COPIA CONTROLADA

Integridad: Principio de seguridad que garantiza la exactitud, completitud y validez de la información, evitando su modificación no autorizada.

Internet: Red mundial de computadoras interconectadas (World Wide Web) que permite el intercambio de información y servicios entre usuarios de diferentes ubicaciones.

Intrusión: Acceso o intento de acceso no autorizado a un activo, sistema o red.

Maltrato: Acciones voluntarias o involuntarias que causan daño a los recursos tecnológicos institucionales, incluyendo descuido o negligencia en su uso.

Malware: Término general para designar programas o códigos maliciosos creados para causar daños, alterar el funcionamiento o sustraer información de sistemas informáticos. Incluye virus, troyanos, spyware, rootkits, backdoors, adware y gusanos.

Mecanismos de seguridad o de control: Controles manuales o automáticos destinados a proteger la información, activos tecnológicos e instalaciones, reduciendo la probabilidad de explotación de vulnerabilidades o mitigando su impacto.

Medios de almacenamiento magnético: Dispositivos utilizados para almacenar información, tales como disquetes, CD, DVD, unidades USB, entre otros.

COPIA CONTROLADA

Módem: Dispositivo electrónico que permite la conexión entre una computadora y una red, convirtiendo las señales digitales en analógicas y viceversa para la transmisión de datos.

Normatividad: Conjunto de lineamientos y disposiciones obligatorias que regulan las actividades dentro de una organización.

Password: Véase **Contraseña**.

Principio de "necesidad de saber": Principio de seguridad según el cual los usuarios deben tener acceso únicamente a la información y recursos necesarios para el desempeño de sus funciones, conforme a sus roles y responsabilidades.

Proceso de Gestión de Tecnologías de la Información: Proceso institucional de la Red de Salud del Centro E.S.E. encargado de la administración, operación y control de las Tecnologías de la Información y las Comunicaciones (TIC).

Respaldo: Copia de seguridad de archivos, datos o configuraciones que permite la recuperación de la información ante una falla o pérdida de los originales.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad de un activo, comprometiendo su seguridad. Generalmente se mide por la probabilidad de ocurrencia y el impacto asociado.

COPIA CONTROLADA

Servidor: Computadora o sistema que proporciona servicios, recursos o información a otras computadoras (clientes) dentro de una red.

Sitio web: Espacio virtual en Internet que agrupa páginas o recursos informativos accesibles mediante una dirección electrónica específica.

Software: Conjunto de programas y documentación asociados que permiten el funcionamiento del hardware y la ejecución de tareas informáticas.

Spyware: Código malicioso diseñado para infiltrarse en un sistema y recopilar información sin autorización del propietario.

User ID: Véase **Identificador de usuario**.

Usuario: Persona que utiliza sistemas, equipos o dispositivos tecnológicos dentro de la organización.

Virus: Programa o código malicioso capaz de replicarse y propagarse a otros sistemas mediante redes o medios de almacenamiento, alterando su funcionamiento.

Vulnerabilidad: Debilidad o brecha de seguridad que puede ser aprovechada por una amenaza para causar daño a un activo, de forma intencional o accidental.

COPIA CONTROLADA

4. MARCO LEGAL

La seguridad informática como conjunto de políticas, procedimientos y herramientas orientadas a proteger la información y los sistemas tecnológicos frente a amenazas internas y externas, tiene como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de los datos, evitando accesos no autorizados, alteraciones indebidas y pérdida de información crítica.

En el sector salud, la seguridad informática adquiere especial relevancia por el manejo de datos sensibles como historias clínicas, resultados diagnósticos y registros administrativos, que deben cumplir con normativas de protección de datos personales y estándares internacionales.

Esta disciplina abarca aspectos como la gestión de accesos, la protección física y lógica de equipos, la seguridad en redes, el cifrado de información, la prevención de incidentes y la continuidad del servicio, incluyendo medidas específicas para entornos de teletrabajo y sistemas en la nube.

Ley 23 de 1981 – Normas sobre ética médica.

Ley 9 de 1979 – Medidas sanitarias y control de calidad en servicios de salud.

Ley 527 de 1999 – Comercio electrónico y firma digital (para historias clínicas electrónicas).

Ley 1273 de 2009 – Modifica el Código Penal colombiano para tipificar delitos informáticos y proteger la integridad de los datos y sistemas.

Ley 1581 de 2012 – Protección de datos personales.

Ley 1751 de 2015 – Ley Estatutaria de Salud (derecho fundamental a la salud).

COPIA CONTROLADA

Decreto 780 de 2016 – Sistema Obligatorio de Garantía de Calidad en Salud.

Resolución 1995 de 1999 – Regula la historia clínica: debe ser única, integral, cronológica y segura. Conservación mínima: 20 años.

Resolución 3100 de 2019 – Condiciones de habilitación de servicios de salud.

Resolución 839 de 2017 – Seguridad del paciente y reporte de eventos adversos.

ISO 27001 – Gestión de seguridad de la información (aplicable a salud). Estándar internacional para la gestión de la seguridad de la información, que establece requisitos para implementar un Sistema de Gestión de Seguridad Informática (SGSI).

COPIA CONTROLADA

5. RESPONSABILIDADES

Rol	Responsabilidad
Gerencia	• Aprobar políticas y recursos
Subgerencia Administrativa y Financiera	• Realizar la aprobación y respaldo institucional • Realizar la Asignación y gestión de recursos • Realizar la supervisión del cumplimiento normativo • Realizar la Gestión de riesgos administrativos • Brindar apoyo a auditorías y controles • Promover la cultura de seguridad • Realizar la coordinación interdependencias • Aplicar medidas disciplinarias en caso de evidenciar incumplimiento
Subgerencia Científica y Subgerencia de Promoción y Mantenimiento de la Salud	• Garantizar el cumplimiento de la seguridad de la información en los procesos asistenciales. • Asegurar la protección de la información clínica y de los datos sensibles. • Supervisar el uso adecuado de los sistemas asistenciales. • Gestionar el riesgo clínico relacionado con la seguridad de la información. • Articular con el área de TI para asegurar la continuidad del servicio asistencial.

Rol	Responsabilidad
	• Controlar el acceso y la conducta del personal asistencial. • Capacitar y sensibilizar al personal asistencial en materia de seguridad. • Gestionar los incidentes de seguridad en el área asistencial. • Acompañar los procesos de auditoría interna y externa.
Gestión del Ambiente Físico	• Garantizar la seguridad física de las instalaciones. • Controlar el acceso a áreas sensibles. • Proteger la infraestructura tecnológica. • Gestionar los riesgos físicos. • Implementar medidas de seguridad perimetral. • Articular con el área de Gestión de Tecnologías y la Información. • Apoyar la continuidad operativa. • Coordinar la gestión de terceros. • Brindar soporte en auditorías.
Seguridad y Salud en el Trabajo	• Integrar la seguridad informática en el Sistema de Gestión SST. • Garantizar condiciones seguras para el uso de equipos y recursos tecnológicos. • Gestionar el riesgo eléctrico y ambiental. • Capacitar y sensibilizar al personal en materia de seguridad y SST. • Gestionar incidentes relacionados con las TIC desde la perspectiva SST. • Coordinar con otras dependencias para la implementación de medidas preventivas. • Supervisar a contratistas y terceros en el cumplimiento de requisitos de seguridad. • Apoyar en la elaboración y ejecución de planes de emergencia y continuidad.
Gestión Humana	• Gestión de ingreso y retiro de personal • Inclusión de la seguridad informática en procesos de selección • Capacitación y sensibilización • Control disciplinario por incumplimiento • Gestión de perfiles y roles organizacionales • Bienestar y aspectos psicosociales • Gestión de contratistas y terceros • Custodia de documentación sensible del personal • Articulación con otras dependencias

COPIA CONTROLADA

Además de lo definido en los apartados anteriores, los directivos, líderes de proceso, coordinadores, jefes y demás funcionarios deberán cumplir de manera estricta las disposiciones establecidas en el presente manual, en coherencia con el DES-PR-002 Programa de Transparencia y Ética Empresarial (PTEE), GHU-PO-001 Código de Conducta y Buen Gobierno Corporativo y el Plan de Desarrollo Institucional 2024–2027.

6. TALENTO HUMANO REQUERIDO

La correcta implementación y sostenibilidad de las políticas y estándares de seguridad informática exige la participación de personal con competencias técnicas, administrativas y operativas, alineadas con los objetivos institucionales. Este talento humano debe garantizar la protección de la información, la continuidad de los servicios y el cumplimiento normativo, mediante la aplicación de controles y buenas prácticas en todos los procesos.

El equipo requerido debe incluir perfiles especializados en tecnologías de la información, seguridad informática, gestión de riesgos, infraestructura física y ambiental, así como personal responsable de la supervisión asistencial y la gestión del talento humano. Cada rol debe contar con formación específica, experiencia comprobada y compromiso con la cultura de seguridad, asegurando la articulación entre áreas para prevenir incidentes, responder eficazmente ante contingencias y promover la mejora continua.

COPIA CONTROLADA

Perfiles y Funciones Clave

Perfil	Competencias	Responsabilidades	Nivel de Formación
Responsable de Seguridad Informática	• Conocimiento avanzado en ciberseguridad y normativas. • Gestión de riesgos. • Liderazgo y toma de decisiones.	• Definir y supervisar políticas de seguridad. • Coordinar planes de contingencia. • Gestionar incidentes críticos.	Profesional en Ingeniería de Sistemas o afines, con especialización o conocimientos comprobados en Seguridad Informática.
Administrador de Sistemas	• Administración de servidores y redes. • Manejo de sistemas operativos y virtualización. • Capacidad analítica.	• Garantizar disponibilidad y rendimiento de sistemas. • Implementar controles de acceso. • Ejecutar copias de seguridad.	Profesional en Ingeniería de Sistemas o Tecnología en Informática.
Responsable de SST (Seguridad y Salud en el Trabajo)	• Conocimiento en normativas SST. • Gestión de riesgos físicos y ambientales. • Comunicación efectiva.	• Integrar seguridad informática en el SG-SST. • Coordinar planes de emergencia. • Supervisar condiciones seguras.	Profesional en Seguridad y Salud en el Trabajo o afines.
Responsable de Talento Humano	• Gestión de personal y procesos disciplinarios. • Conocimiento en normativas laborales. • Habilidades de liderazgo.	• Incluir seguridad informática en procesos de selección. • Gestionar ingreso y retiro de personal. • Custodiar documentación sensible.	Profesional en Administración, Psicología Organizacional o afines.

COPIA CONTROLADA

7. MATERIALES, INSUMOS Y EQUIPOS REQUERIDOS

Para garantizar la correcta implementación de las políticas y estándares de seguridad informática, se requiere contar con los siguientes recursos tecnológicos y operativos:

- **Equipos de cómputo**: estaciones de trabajo, portátiles y dispositivos autorizados para el personal.
- **Infraestructura de red:** cableado estructurado, dispositivos de conectividad (switches, routers, firewalls) y sistemas de monitoreo.
- **Servicios de comunicación**: plataformas de correo electrónico institucional, herramientas de colaboración y mensajería segura.
- **Sistemas de respaldo y almacenamiento**: soluciones para copias de seguridad y protección de datos críticos.
- **Elementos de seguridad física:** cerraduras electrónicas, cámaras de vigilancia y controles de acceso a áreas restringidas.

COPIA CONTROLADA

8. CONTENIDO

8.1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

8.1.1. Política corporativa de seguridad de la información

En la Red de Salud del Centro, la información constituye un activo esencial para la prestación eficiente de los servicios y para la toma de decisiones acertadas. Por esta razón, la organización mantiene un compromiso expreso con la protección de sus activos informacionales más relevantes, como parte de una estrategia orientada a la continuidad del negocio, la gestión de riesgos y la consolidación de una cultura institucional de seguridad.

Todos los usuarios de bienes y servicios informáticos deberán conducirse conforme a los principios de confidencialidad de la información, uso responsable de los recursos tecnológicos y cumplimiento estricto de lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios de la Red de Salud del Centro.

8.1.2. Responsabilidades de los usuarios

Es responsabilidad de todos los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática establecidos por la Red de Salud del Centro, contenidos en el presente manual.

Cada usuario deberá conocer, aplicar y promover el cumplimiento de estas políticas en el ámbito de sus funciones, reportando cualquier situación que pueda representar un riesgo para la seguridad de la información o los sistemas institucionales.

8.1.3. Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos de la Red de Salud del Centro ESE deberán actuar conforme a los principios de confidencialidad, integridad y uso adecuado de los recursos informáticos y de información.

COPIA CONTROLADA

El acceso a los sistemas institucionales implica la aceptación de los compromisos y responsabilidades descritos en los acuerdos de uso y confidencialidad establecidos por la organización. Diligenciar (cuando aplique) el formato GTI-F-031 Compromiso De Confidencialidad, Propiedad Intelectual y Aceptación de Políticas de Seguridad y Privacidad de la Información.

8.1.4. Entrenamiento en seguridad informática

Todo funcionario, contratista o afiliado partícipe que ingrese a la Red de Salud del Centro deberá:

- Leer y comprender el Manual de Políticas y Estándares de Seguridad Informática para Usuarios, disponible en el sitio web institucional **www.esecentro.gov.co**, en el aplicativo documental "Almera**"**, y en los escritorios de los equipos de cómputo corporativos.

- Cumplir las obligaciones allí descritas y conocer las sanciones aplicables en caso de incumplimiento.

- Participar en las actividades de capacitación y concienciación en seguridad informática organizadas por el Proceso de Gestión de Tecnologías de la Información.

COPIA CONTROLADA

8.1.5. Medidas disciplinarias

Cuando el Proceso de Gestión de Tecnologías y la Información identifique el incumplimiento de las disposiciones establecidas en el presente manual, deberá emitir el reporte o denuncia correspondiente ante la instancia competente, para que se apliquen las medidas y sanciones que procedan conforme a la normativa institucional y legal vigente.

8.2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Los mecanismos de control y acceso físico, aplicables tanto al personal interno como a terceros, deben garantizar que únicamente las personas debidamente autorizadas ingresen a las instalaciones y áreas restringidas de la Red de Salud del Centro. Este control tiene como finalidad proteger los equipos de cómputo, los sistemas de comunicación y demás activos tecnológicos e infraestructurales, asegurando la integridad y continuidad de los servicios.

8.2.1. Resguardo y protección de la información

8.2.1.1. Reporte inmediato de incidentes.

El usuario deberá reportar de forma inmediata al Proceso de Gestión de Tecnologías y la Información cualquier situación que represente un riesgo real o potencial para los equipos de

COPIA CONTROLADA

cómputo o de comunicaciones, tales como robos, sabotajes, fugas de agua, conatos de incendio u otros incidentes.

8.2.1.2. Custodia de medios y dispositivos.

El usuario tiene la obligación de proteger y custodiar los medios de almacenamiento y dispositivos bajo su administración (CDs, DVDs, memorias USB, discos externos, computadores y portátiles) que contengan información reservada o confidencial.

8.2.1.3. Restricción y control de dispositivos extraíbles.

El uso de dispositivos de almacenamiento extraíbles estará restringido mediante los puertos USB de los equipos propiedad o en alquiler de la Red de Salud del Centro. Solo se permitirán excepciones autorizadas por la Gerencia y el Proceso de Gestión de Tecnologías y la Información, debidamente documentadas.

El usuario debe realizar mediante el antivirus institucional un análisis previo de todo dispositivo que pretenda conectar a un equipo de cómputo, independientemente del tipo de puerto utilizado, con el fin de garantizar su integridad y cumplimiento de las políticas de seguridad establecidas.

8.2.1.4. Prevención de fuga de información.

Es responsabilidad del usuario prevenir cualquier fuga o divulgación no autorizada de la información institucional almacenada en los equipos de cómputo asignados.

COPIA CONTROLADA

8.2.2. Controles de acceso físico

8.2.2.1. Registro y control de dispositivos externos.

Todo dispositivo tecnológico que no sea propiedad de la Red de Salud del Centro y que ingrese a cualquiera de las IPS deberá ser registrado en las bitácoras del personal de seguridad. En caso de que dicho dispositivo permanezca en las instalaciones por más de un día hábil, será obligatoria la emisión de una orden de salida, la cual deberá contar con el visto bueno del Proceso de Gestión de Tecnologías y la Información.

8.2.3. Seguridad en áreas de trabajo

Los centros de datos y áreas críticas de la Red de Salud del Centro son zonas de acceso restringido. Solo el personal autorizado por el Proceso de Gestión de Tecnologías y la Información podrá ingresar a estas áreas, conforme a los procedimientos de control establecidos.

8.2.4. Copias de Seguridad

La Red de Salud del Centro deberá garantizar que toda la información institucional clasificada almacenada en servidores, dispositivos de red, estaciones de trabajo y otros medios tecnológicos sea respaldada periódicamente mediante mecanismos que aseguren su identificación, integridad, protección y disponibilidad. Asimismo, se deberá contar con un plan de restauración de copias de seguridad, probado a intervalos regulares para garantizar su confiabilidad en caso de contingencia, y con políticas claras sobre los periodos de retención de los respaldos.

COPIA CONTROLADA

El Proceso de Gestión de Tecnologías y la Información es responsable de definir y ejecutar los procedimientos de resguardo y recuperación, incluyendo la frecuencia, traslado, identificación y ubicación de los medios de almacenamiento. Los medios magnéticos con información crítica deberán almacenarse en la dependencia designada por el Proceso de Gestión Documental, bajo condiciones de seguridad física y ambiental apropiadas.

8.2.4.1. **Copias de seguridad programadas**.

A los equipos de cómputo del área administrativa y a los del área asistencial que lo requieran se les realizará copia de seguridad de las carpetas “Mis Documentos” y “Escritorio”, según la programación definida por el Proceso de Gestión de Tecnologías y la Información. La información almacenada fuera de estas ubicaciones no será respaldada y quedará bajo **responsabilidad del usuario.**

8.2.4.2. **Solicitud formal de recuperación.**

La recuperación de información deberá solicitarse mediante documento formal al Proceso de Gestión de Tecnologías y la Información, con el visto bueno del líder de proceso.

8.2.5. Energía Regulada

8.2.5.1. **Uso exclusivo de tomas reguladas.**

La Red de Salud del Centro dispone de alimentación eléctrica regulada exclusivamente para los equipos de cómputo y comunicaciones. Está prohibido conectar a estos puntos (tomas de

COPIA CONTROLADA

color naranja) dispositivos no autorizados como celulares, ventiladores, radios, cafeteras, impresoras láser u otros aparatos eléctricos.

8.2.5.2. Encendido durante jornada laboral.

Con el fin de contribuir al ahorro energético y la sostenibilidad ambiental, los equipos deberán permanecer encendidos únicamente durante la jornada laboral.

8.2.5.3. Apagado y reinicio de equipos

Antes de retirarse del puesto de trabajo, el usuario deberá apagar correctamente todos los dispositivos (CPU, monitor e impresora). En los casos de cambio de turno, el equipo deberá reiniciarse en el momento de la entrega.

8.2.6. Acceso remoto

8.2.6.1. Acceso Remoto Seguro.

Los usuarios que requieran conectarse remotamente a la infraestructura tecnológica de la Red de Salud del Centro deberán utilizar únicamente los mecanismos de acceso remoto autorizados por el Proceso de Gestión de Tecnologías y la Información, los cuales deben incluir controles de autenticación y cifrados seguros.

COPIA CONTROLADA

8.2.6.2. Restricción de Dispositivos Móviles Personales.

No está permitida la conexión de dispositivos móviles personales (smartphones, tabletas, Asistentes Digitales, etc.) a los recursos tecnológicos institucionales, salvo autorización expresa del área competente.

8.2.7. Redes Inalámbricas (Wi-Fi)

La red inalámbrica institucional es una extensión de la red local que permite el acceso controlado a Internet y a los servicios informáticos de la Red de Salud del Centro. Este servicio es de uso exclusivo para fines laborales y está destinado únicamente a funcionarios y colaboradores autorizados.

Los dispositivos que requieran conexión inalámbrica deberán solicitar por medio de RING en la subactividad de Redes y Datos en el formulario instalación puntos de red o zona wifi para registrar su dirección MAC en la plataforma tecnológica institucional. Si tienen invitados y requieren wifi se deberá solicitar por medio de RING en la subactividad de Redes y Datos en el formulario solicitud voucher para red wifi invitados, en este se le asignará un código por unos días.

La solicitud de registro deberá ser avalada por el líder de proceso y tramitada ante el Proceso de Gestión de Tecnologías y la Información.

COPIA CONTROLADA

Está prohibido utilizar las redes inalámbricas para actividades no laborales como reproducción de música, videos o descargas de contenido multimedia.

8.2.8. Fondo de Escritorio y Protector de Pantalla

Los equipos institucionales utilizan fondos de escritorio y protectores de pantalla corporativos, destinados a difundir información institucional. No está permitido modificar, eliminar o sustituir estos elementos en los equipos de cómputo.

8.2.9. Protección y ubicación de los equipos

8.2.9.1. Autorización para mover o instalar equipos.

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de estos sin la autorización del Proceso de Gestión de Tecnologías y la Información, debiéndose solicitar a la misma en caso de requerir este servicio.

8.2.9.2. Registro y control de equipos informáticos.

El proceso de Ambiente Físico a través del responsable de Activos Fijos de la Red de Salud del Centro E.S.E debe generar el documento de resguardo, obtener la firma del usuario asignado y garantizar que los equipos informáticos permanezcan en la ubicación autorizada por el departamento de Gestión de Tecnologías y la Información.

COPIA CONTROLADA

8.2.9.3. Uso exclusivo para funciones laborales.

El equipo de cómputo asignado se destinará exclusivamente a las funciones propias del usuario dentro de la Red de Salud del Centro E.S.E. y únicamente se almacenará información relacionada con el ejercicio de dichas funciones.

8.2.9.4. Solicitud de capacitación en herramientas.

Corresponde al usuario solicitar la capacitación necesaria para el manejo adecuado de las herramientas informáticas utilizadas en su equipo, con el fin de prevenir riesgos derivados de un uso incorrecto y optimizar su aprovechamiento.

8.2.9.5. Almacenamiento en directorios respaldados.

Es responsabilidad del usuario almacenar su información únicamente en las carpetas “Escritorio” y “Mis Documentos”, que son los directorios de trabajo recomendados y cuentan con copia de seguridad programada.

8.2.9.6. Entorno de trabajo limpio y seguro.

Los usuarios deberán mantener un entorno de trabajo limpio, ordenado y seguro.

- Evitar consumir alimentos o bebidas cerca del equipo.
- Evitar colocar objetos sobre el equipo o bloquear los orificios de ventilación del monitor y la CPU.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad
- Asegurarse de que los cables de conexión no queden pisados ni aplastados por objetos colocados encima o contra ellos.

COPIA CONTROLADA

- Cuando sea necesario realizar cambios múltiples en el equipo de cómputo debido a la reubicación de puestos de trabajo, estos deberán notificarse al Proceso de Gestión de Tecnologías y la Información con una anticipación mínima de tres días hábiles, mediante un plan detallado de movimientos debidamente autorizado por el titular del área correspondiente.
- Se prohíbe al usuario abrir o desarmar los equipos de cómputo, ya que esta acción lo hace responsable de cualquier daño que pueda ocasionarse.

8.2.10. Mantenimiento de Equipo

8.2.10.1. Instalación y Mantenimiento Autorizado.

Únicamente el personal perteneciente al Proceso de Gestión de Tecnologías y la Información y proveedores debidamente autorizados podrán llevar a cabo los servicios y reparaciones al equipo informático.

8.2.10.2. Prohibición de instalación y uso indebido de cuentas.

Ningún colaborador debe realizar tareas de instalación de equipos, programas (software) o reparaciones, incluso si cuenta con capacitación técnica o profesional, ya que estas acciones requieren una cuenta de administrador. Obtenerla de manera irregular constituye una falta grave. Dichas actividades son responsabilidad exclusiva del personal contratado para el mantenimiento.

COPIA CONTROLADA

8.2.10.3. Resguardo Previo a Mantenimiento.

Los usuarios deben informar sobre la información que consideren relevante cuando el equipo sea enviado a reparación y asegurarse de respaldar aquella información sensible que se encuentre en el equipo, para prevenir la pérdida involuntaria derivada del proceso de reparación. Para ello, deberán solicitar la asesoría del personal del Proceso de Gestión de Tecnologías y la Información.

8.2.10.4. Reporte inmediato de fallas.

Cuando el colaborador responsable de un equipo de cómputo detecte problemas en su funcionamiento, ya sea a nivel lógico o físico, deberá informar de inmediato al líder del proceso para que se realice la verificación correspondiente y se emita un diagnóstico que indique las acciones necesarias para corregir la falla o gestionar la reparación.

8.2.10.5. Programación de mantenimientos preventivos.

El Proceso de Gestión de Tecnologías y la Información programará el mantenimiento preventivo de los equipos de cómputo de la Red de Salud del Centro E.S.E dos veces al año. Para ello, elaborará y comunicará los cronogramas con la debida anticipación. El usuario deberá facilitar su equipo en la fecha y hora indicadas en dicho cronograma.

8.2.11. Pérdida o Transferencia de Equipo

8.2.11.1. Responsabilidad del usuario sobre el equipo bajo su custodia

Cada usuario es responsable del equipo bajo su custodia y deberá responder por su pérdida o daño conforme a la normatividad vigente.

COPIA CONTROLADA

8.2.11.2. Carácter personal e intransferible del resguardo de equipos portátiles

El resguardo de los equipos portátiles asignados es una responsabilidad exclusiva del usuario, quien deberá garantizar su cuidado y protección en todo momento. Esta obligación implica evitar la cesión, préstamo o transferencia del equipo a terceros, así como adoptar las medidas necesarias para prevenir daños, pérdida o uso indebido. El incumplimiento de esta disposición podrá generar responsabilidades conforme a los lineamientos institucionales vigentes.

8.2.11.3. Procedimiento ante pérdida, robo o extravío del equipo o accesorios

Ante la pérdida, robo o extravío del equipo o accesorios, el usuario deberá reportar inmediatamente el incidente al Proceso de Gestión de Tecnologías y la Información, a través del correo electrónico utilizando el formato GAF-F-061 Reporte de pérdida por daño, hurto o extravío de activos. Además, tener en cuenta el GAF-P-018 Procedimiento para el Manejo de pérdida por daño, hurto o extravío de activos

8.2.12. Uso de dispositivos especiales

El usuario asignado como responsable de dispositivos especiales, tales como grabadores, quemadores de discos u otros equipos similares, deberá garantizar su utilización conforme a las políticas institucionales y a los fines autorizados. Esto implica:

- **Cumplimiento Normativo**: Asegurar que el uso se limite exclusivamente a actividades aprobadas, evitando cualquier práctica que pueda comprometer la seguridad o integridad de la información. El uso de grabadores o quemadores de discos está limitado exclusivamente a actividades de respaldo de información institucional.

COPIA CONTROLADA

- **Protección física y lógica**: Mantener los dispositivos en condiciones óptimas, prevenir daños y aplicar medidas de seguridad para evitar accesos no autorizados.
- **Responsabilidad ante incidentes**: Reportar de forma inmediata cualquier anomalía, pérdida, mal funcionamiento o uso indebido al área correspondiente, asumiendo las consecuencias establecidas por la organización.

8.2.13. Daño del equipo

Todo equipo de cómputo o recurso tecnológico que sufra daños como consecuencia de maltrato, descuido o negligencia por parte del usuario deberá ser reparado o reemplazado a su cargo. Esta acción se realizará conforme al dictamen técnico emitido por el Proceso de Gestión de Tecnologías y la Información, el cual determinará la naturaleza del daño y las medidas correctivas necesarias.

8.3. POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Los usuarios deben utilizar los mecanismos institucionales establecidos para proteger la información que reside y se utiliza en la infraestructura tecnológica de la Red de Salud del Centro ESE. Asimismo, deben salvaguardar la información reservada o confidencial que, por necesidades institucionales, deba ser almacenada o transmitida, ya sea dentro de la red interna o hacia redes externas como Internet.

COPIA CONTROLADA

Los usuarios que hagan uso de equipos de cómputo deben conocer y aplicar las medidas necesarias para prevenir la presencia de código malicioso (virus, malware, spyware, entre otros). En caso de requerir orientación, podrán acudir al Proceso de Gestión de Tecnologías y la Información o a su representante en la comuna correspondiente.

8.3.1. Uso de medios de almacenamiento

8.3.1.1. Autorización para uso de almacenamiento compartido

Toda solicitud para utilizar un medio de almacenamiento compartido deberá contar con la autorización del titular del área propietaria de la información y ajustarse estrictamente a las directrices institucionales. En ningún caso estos medios podrán emplearse como depósitos permanentes de archivos, garantizando así la correcta administración y seguridad de la información.

8.3.1.2. Requisitos de la solicitud

La solicitud para el uso de medios compartidos deberá especificar claramente los fines de utilización y presentarse con la firma del líder del proceso involucrado, así como del líder del Proceso de Gestión de Tecnologías y la Información, asegurando trazabilidad y responsabilidad en la autorización.

8.3.1.3. Respaldo periódico de información crítica

El Proceso de Gestión de Tecnologías y la Información realizará respaldos periódicos de la información sensible y crítica almacenada en equipos institucionales y carpetas autorizadas,

COPIA CONTROLADA

con el objetivo de garantizar la continuidad operativa y la protección de datos ante posibles incidentes.

8.3.1.4. Autorización para respaldos externos

Cualquier respaldo de información hacia un medio externo deberá ser solicitado y autorizado por escrito al Proceso de Gestión de Tecnologías y la Información, evitando riesgos de fuga de datos y asegurando el cumplimiento de las políticas de seguridad institucional.

8.3.1.5. Conservación de registros y documentos

Los colaboradores deberán conservar los registros y documentos activos, así como aquellos clasificados como reservados o confidenciales, conforme a las disposiciones aplicables a su cargo, garantizando la integridad y disponibilidad de la información institucional.

8.3.1.6. Registro y auditoría de actividades

Todas las actividades realizadas por los usuarios dentro de la infraestructura tecnológica son registradas y están sujetas a procesos de auditoría, con el fin de asegurar la transparencia, el cumplimiento normativo y la protección de los recursos tecnológicos.

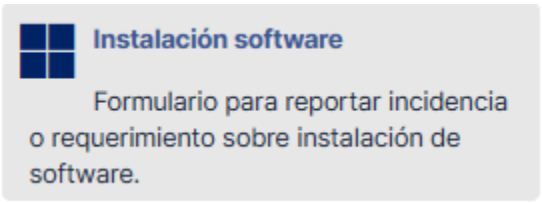
8.3.2. Instalación de software

Control y autorización para instalación de programas

COPIA CONTROLADA

8.3.2.1. Solicitud y justificación

Los usuarios que requieran instalar software no propiedad de la Red de Salud del Centro deberán justificar su necesidad mediante solicitud escrita dirigida al Proceso de Gestión de Tecnologías y la Información, firmada por el líder del proceso. La solicitud debe incluir el equipo donde se instalará, el periodo de uso y la factura de compra del programa. Esta solicitud se realiza a través del formulario de RING "Instalación Software"



8.3.2.2. Desinstalación inmediata sin factura

Si no se presenta la factura correspondiente, el personal autorizado procederá a desinstalar el software de forma inmediata, garantizando el cumplimiento de las políticas institucionales.

8.3.2.3. Prohibición de instalación no autorizada

Se considera falta grave instalar cualquier programa en equipos de la Red (incluidos servidores, dispositivos móviles o cámaras) sin la autorización expresa del Proceso de Gestión de Tecnologías y la Información.

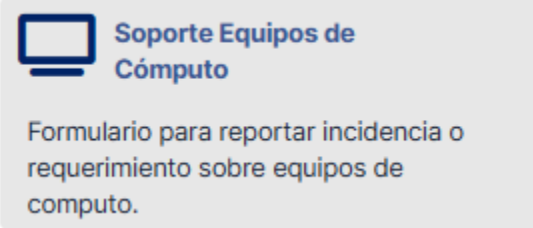
8.3.3. Identificación de incidentes

Reporte oportuno de incidentes de seguridad

COPIA CONTROLADA

8.3.3.1. Reporte inmediato de sospechas

Todo usuario que detecte o sospeche un incidente de seguridad informática deberá reportarlo de inmediato al Proceso de Gestión de Tecnologías y la Información o al encargado de la comuna, indicando los motivos del reporte, a través de la plataforma RING – Soporte Equipos de Cómputo



8.3.3.2. Notificación de revelación de información

Si se sospecha o confirma la revelación, modificación o eliminación no autorizada de información confidencial o reservada, el usuario deberá notificarlo a su líder de proceso para activar las medidas correspondientes.

8.3.3.3. Incidentes en operación de activos tecnológicos

Cualquier incidente generado durante la utilización u operación de los activos tecnológicos deberá ser informado al Proceso de Gestión de Tecnologías y la Información para su análisis y resolución.

8.3.4. Administración de la configuración

Restricciones en la configuración de redes y protocolos. Los usuarios no deben establecer redes locales, conexiones remotas ni intercambiar información mediante FTP u otros protocolos

COPIA CONTROLADA

sin autorización escrita del Proceso de Gestión de Tecnologías y la Información, quien mantendrá los registros correspondientes.

8.3.5. Seguridad de la red

Protección contra actividades no autorizadas. Toda actividad no autorizada que implique exploración, escaneo o pruebas de vulnerabilidad sobre la red de datos o sus aplicaciones será considerada un ataque informático y constituirá falta grave. El Proceso de Gestión de Tecnologías y la Información podrá suspender o eliminar el acceso de cualquier usuario sin previo aviso cuando sea necesario para garantizar la disponibilidad, integridad o seguridad de los servicios, o durante investigaciones por posibles violaciones a las políticas de seguridad.

8.3.6. Uso del correo electrónico institucional

Lineamientos para un uso seguro y responsable del correo corporativo

8.3.6.1. Uso adecuado de cuentas institucionales

Cada usuario debe utilizar únicamente su cuenta de correo institucional asignada, garantizando la correcta gestión y protección de la información. En caso de ausencia, el titular podrá redireccionar su correo interno a otra cuenta institucional autorizada, asegurando siempre la confidencialidad y el cumplimiento de las políticas de seguridad.

COPIA CONTROLADA

8.3.6.2. Propiedad y conservación de mensajes

Los buzones y mensajes son propiedad de la institución. El usuario debe conservar únicamente aquellos relacionados con sus funciones laborales, evitando almacenar información personal o irrelevante.

8.3.6.3. Envío seguro de información confidencial

El envío de información reservada o confidencial solo podrá realizarse mediante el correo institucional y a destinatarios autorizados, asegurando el cumplimiento de las políticas de seguridad. Toda información reservada o confidencial cuyo destinatario sea una parte interesada externa deberá contar con el aval de la gerencia y gestión jurídica y contractual.

8.3.6.4. Acceso por orden judicial o investigación

La institución podrá acceder o revelar mensajes institucionales en cumplimiento de una orden judicial o durante investigaciones por violación de políticas de seguridad informática.

8.3.6.5. Uso exclusivo para fines laborales

El correo institucional debe utilizarse únicamente para actividades laborales. El tamaño del buzón será definido por el Proceso de Gestión de Tecnologías y la Información según las necesidades del usuario.

8.3.6.6. Creación de cuentas externas

La creación de cuentas de correo externas requerirá solicitud escrita con visto bueno del líder del proceso y autorización del Proceso de Gestión de Tecnologías y la Información.

COPIA CONTROLADA

8.3.6.7. Prohibición de suplantación de identidad

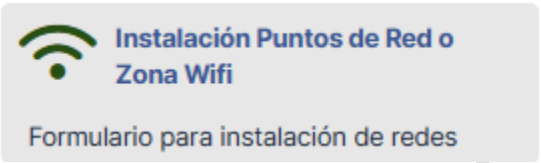
Queda estrictamente prohibido falsear, ocultar o suplantar la identidad en el uso del correo electrónico institucional.

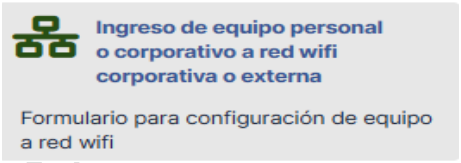
8.3.7. Uso y acceso a Internet

Lineamientos para la navegación segura y controlada.

8.3.7.1. Solicitud de ampliación o modificación

Cualquier solicitud de ampliación o modificación del servicio deberá realizarse por escrito y contar con las respectivas autorizaciones a través de RING.



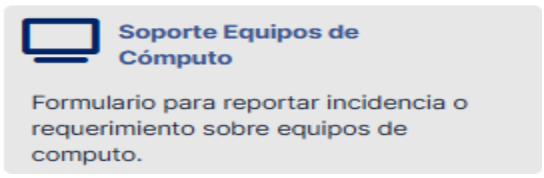


8.3.7.2. Acceso solo por canales institucionales

Todos los accesos a Internet deben realizarse exclusivamente a través de los canales institucionales, evitando el uso de medios no autorizados.

8.3.7.3. Reporte inmediato de incidentes

Los incidentes de seguridad detectados durante la navegación deben reportarse de forma inmediata al área responsable.



COPIA CONTROLADA

8.3.7.4. Autorización para accesos no convencionales

Cualquier acceso mediante canales no convencionales requerirá autorización escrita.

Niveles de acceso a Internet:

- **Nivel 1:** Sin restricciones.
- **Nivel 2:** Internet y mensajería restringidos.
- **Nivel 3:** Internet restringido.
- **Nivel 4:** Sin acceso a Internet.

8.3.7.5. Acciones no permitidas

- Acceder a páginas de contenido inapropiado, ilegal o no ético.
- Realizar compras, descargas o actividades personales.
- Utilizar redes sociales o servicios de mensajería con fines no laborales.
- Descargar juegos, música, películas o software no autorizado.
- Descargar material audiovisual sin aprobación previa del Proceso de Gestión de Tecnologías y la Información.

8.4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Cada usuario es responsable del mecanismo de control de acceso que le sea asignado, esto es, su nombre de usuario (UserID) y contraseña (Password) necesarios para acceder a la información y a la infraestructura tecnológica de la Red de Salud del Centro. Por tanto, deberá mantenerlos en estricta confidencialidad. El Proceso de Gestión de Tecnologías y la Información es el único autorizado para otorgar accesos a la información y recursos

COPIA CONTROLADA

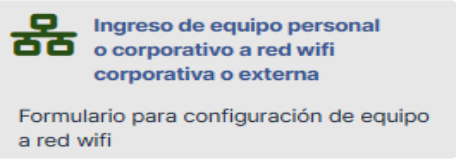
tecnológicos, asignando los permisos mínimos indispensables para el cumplimiento de las funciones del usuario, conforme al principio de “necesidad de saber”.

8.4.1. Controles de acceso lógico

Lineamientos para el acceso seguro a la infraestructura tecnológica.

8.4.1.1. Autorización para personal externo

El acceso a la infraestructura tecnológica por parte de personal externo deberá ser autorizado, al menos, por un líder de proceso o un subgerente, mediante oficio dirigido al Proceso de Gestión de Tecnologías y la Información, quien realizará la habilitación correspondiente.



8.4.1.2. Uso legítimo de la infraestructura

La infraestructura tecnológica debe utilizarse únicamente para fines autorizados. Está prohibido intentar obtener accesos no permitidos a información o sistemas institucionales.

8.4.1.3. Responsabilidad sobre credenciales

Cada usuario es responsable del uso y custodia de su identificador y contraseña, evitando cualquier práctica que comprometa su seguridad. Cabe resaltar que es de índole personal e intransferible. Cada usuario debe contar con un identificador único e intransferible. No se permite compartir identificadores entre varios usuarios.

COPIA CONTROLADA

8.4.1.4. Autenticación obligatoria

Antes de utilizar cualquier recurso tecnológico institucional, los usuarios deberán autenticarse mediante los mecanismos de control de acceso provistos por el Proceso de Gestión de Tecnologías y la Información.

8.4.1.5. Confidencialidad de mecanismos de acceso

No se debe proporcionar información sobre mecanismos de acceso lógico a personal externo, salvo autorización expresa del Proceso de Gestión de Tecnologías y la Información.

8.4.1.6. Prohibición de compartir credenciales

Está prohibido compartir las credenciales de acceso. Cualquier acción realizada con un identificador y contraseña será responsabilidad exclusiva del titular, salvo comprobación de suplantación o usurpación.

8.4.2. Administración de privilegios

Gestión segura de roles y permisos.

8.4.2.1. Comunicación de cambios

Cualquier modificación en roles o funciones que implique cambios en privilegios de acceso debe comunicarse por escrito o vía correo institucional al Proceso de Gestión de Tecnologías y la Información, con visto bueno del líder de proceso o subgerente.

COPIA CONTROLADA

8.4.3. Administración y uso de contraseñas

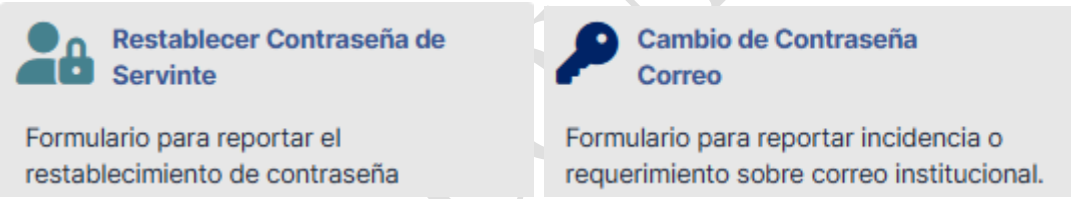
Políticas para la gestión segura de contraseñas.

8.4.3.1. Asignación individual

Las contraseñas de acceso a la red o sistemas serán asignadas de forma individual. Está prohibido el uso compartido de contraseñas.

8.4.3.2. Reporte de incidencias

En caso de olvido, bloqueo o extravío de la contraseña, el usuario deberá reportarlo mediante RING (intranet), especificando si corresponde al acceso de red o de sistemas, para que se genere una nueva.



8.4.3.3. Obtención segura

Para obtener o cambiar una contraseña, el usuario debe acreditarse ante el Proceso de Gestión de Tecnologías y la Información como colaborador activo.

8.4.3.4. Prohibición de credenciales visibles

Está prohibido mantener credenciales visibles en medios impresos o escritos dentro del área de trabajo.

COPIA CONTROLADA

8.4.3.5. Criterios mínimos de seguridad

Las contraseñas deben cumplir con los siguientes criterios mínimos:

- No contener secuencias numéricas consecutivas.
- Tener al menos ocho (8) caracteres alfanuméricos (letras y números).
- Ser difíciles de adivinar y no relacionarse con datos personales o laborales.
- Diferir de las contraseñas usadas previamente.

8.4.3.6. Cambio solo por el titular

La contraseña podrá ser modificada únicamente a solicitud del titular de la cuenta.

8.4.3.7. Cambio inmediato ante sospecha

Si se sospecha que la contraseña ha sido comprometida, el usuario debe solicitar su cambio de inmediato.

8.4.3.8. Prohibición de almacenamiento automático

Está prohibido almacenar contraseñas en programas o sistemas que ofrezcan la opción de "recordar contraseña".

8.4.3.9. Solicitud formal para cambios

Toda solicitud de cambio o desbloqueo de contraseña deberá presentarse mediante oficio firmado por el líder de proceso del usuario solicitante.

COPIA CONTROLADA

8.4.4. Control de accesos remotos

Regulación del acceso externo a la red institucional.

8.4.4.1. Autorización para acceso externo

Está prohibido acceder a la red institucional desde redes externas sin autorización. Las excepciones deben documentarse y contar con visto bueno de la Gerencia o del Proceso de Gestión de Tecnologías y la Información.

8.4.4.2. Administración remota segura

No se permite la administración remota de equipos conectados a Internet, salvo con autorización expresa y mediante mecanismos seguros validados por la Red de Salud del Centro ESE.

8.5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

8.5.1. Derechos de propiedad intelectual

Protección del software y desarrollos tecnológicos.

8.5.1.1. Prohibición de copias no autorizadas

Está prohibida la reproducción o copia no autorizada de software adquirido o desarrollado por la Red de Salud del Centro ESE, en cumplimiento de las leyes de derechos de autor y políticas institucionales.

COPIA CONTROLADA

8.5.1.2. Propiedad de desarrollos tecnológicos

Todo sistema o desarrollo tecnológico realizado por personal interno o externo bajo la coordinación del Proceso de Gestión de Tecnologías y la Información será considerado propiedad intelectual de la Red de Salud del Centro ESE.

8.5.2. Revisiones del cumplimiento

Monitoreo y control de políticas de seguridad.

8.5.2.1. Auditorías periódicas

El Proceso de Gestión de Tecnologías y la Información realizará revisiones periódicas para verificar el cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

8.5.2.2. Mecanismos de control y reporte

Se podrán implementar mecanismos para monitorear el uso de recursos informáticos y detectar posibles usos indebidos, los cuales serán reportados y tratados según las disposiciones vigentes.

8.5.2.3. Cumplimiento obligatorio

El conocimiento y cumplimiento de este manual es obligatorio para todos los usuarios de equipos de cómputo de la Red de Salud del Centro ESE. Su desconocimiento no exime de responsabilidad ni podrá alegarse como justificación ante una infracción.

COPIA CONTROLADA

8.5.3. Violaciones de seguridad informática

Acciones prohibidas para proteger la integridad de los sistemas.

8.5.3.1. Prohibición de herramientas para vulnerar seguridad

Está prohibido el uso de herramientas de hardware o software destinadas a vulnerar los controles de seguridad informática, salvo autorización expresa del Proceso de Gestión de Tecnologías y la Información.

8.5.3.2. Restricción de pruebas no autorizadas

Ningún funcionario podrá realizar pruebas sobre los controles o sistemas de la Red, salvo que cuente con autorización formal del Proceso de Gestión de Tecnologías y la Información o de los órganos fiscalizadores competentes.

8.5.3.3. Prohibición de explotación de vulnerabilidades

Está prohibido probar, explotar o divulgar vulnerabilidades de seguridad, salvo en pruebas controladas y aprobadas por la instancia competente.

8.5.3.4. Prohibición de código malicioso

Se prohíbe crear, propagar o ejecutar virus, malware, spyware u otros programas que afecten el desempeño, disponibilidad o integridad de los sistemas de información.

COPIA CONTROLADA

8.5.3.5. Restricción de navegación privada

No está permitido utilizar el modo incógnito, modo privado o funcionalidades similares en navegadores instalados en equipos institucionales.

8.5.3.6. Configuración obligatoria de navegadores

Los navegadores deben permanecer configurados para registrar el historial de navegación, cookies, caché y demás datos requeridos para los procesos de auditoría y monitoreo.

8.5.3.7. Prohibición de alteración de controles

Los usuarios no están autorizados a modificar configuraciones, instalar complementos, extensiones o realizar cualquier acción que permita evadir, deshabilitar o alterar los controles de registro y seguimiento de los navegadores.

8.6. POLÍTICAS Y ESTÁNDARES DEL TELETRABAJO

8.6.1. Generalidades

El teletrabajo, también conocido como trabajo remoto, flexible o desde casa, es una modalidad de organización laboral promovida en Colombia desde el año 2008 mediante la **Ley 1221**, reglamentada posteriormente por el **Decreto 884 de 2012**.

De acuerdo con esa normativa, el teletrabajo consiste en la ejecución de actividades remuneradas o la prestación de servicios utilizando como soporte las Tecnologías de la

COPIA CONTROLADA

Información y la Comunicación (TIC), sin requerir la presencia física del trabajador en un lugar específico de trabajo. Puede desarrollarse en modalidades autónoma, móvil o suplementaria. A diferencia del trabajo presencial, el teletrabajo implica nuevos desafíos en materia de seguridad informática y protección de datos, dado que los equipos y redes domésticas no cuentan con los mismos estándares corporativos de seguridad.

Por tanto, resulta esencial garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Las siguientes políticas establecen los lineamientos mínimos de ciberseguridad que deberán cumplir los funcionarios y contratistas autorizados para realizar teletrabajo.

8.6.2. Políticas generales para el teletrabajo

El personal que desarrolle sus actividades laborales mediante teletrabajo deberá aplicar las siguientes reglas básicas de seguridad informática, con el fin de evitar la exposición de datos personales o institucionales:

- Utilizar únicamente los canales y plataformas corporativas aprobadas por la entidad.
- Mantener actualizado el software y sistemas de protección del equipo.
- Evitar el almacenamiento de información institucional en dispositivos personales.
- Aplicar las normas del presente manual y las disposiciones de la Ley 1581 de 2012 sobre protección de datos personales.

COPIA CONTROLADA

8.6.3. Redes WiFi

Cuando se maneje información confidencial o sensible de la Red de Salud del Centro, el usuario deberá:

- Conectarse exclusivamente a redes privadas y seguras, preferiblemente la red doméstica propia o la red privada corporativa (VPN).
- Abstenerse de utilizar redes WiFi públicas (cafeterías, parques, aeropuertos, etc.), por su alto riesgo de interceptación de datos.
- Emplear una Red Privada Virtual (VPN) para cifrar la conexión y proteger la información transmitida.

8.6.4. Sistema operativo y seguridad del equipo

Los equipos utilizados para el teletrabajo deberán cumplir con los siguientes requisitos:

- **Actualizar periódicamente el sistema operativo y las aplicaciones**, a fin de corregir vulnerabilidades.
- **Instalar y mantener activo un antivirus actualizado**, que detecte y bloquee software malicioso.
- **Usar contraseñas seguras** y cambiarlas regularmente.
- **Utilizar exclusivamente el correo corporativo** para asuntos laborales, evitando el uso del correo personal.

8.6.5. Pérdida o robo del dispositivo

En caso de pérdida o robo del dispositivo utilizado para el teletrabajo, el usuario deberá:

- Denunciar el hecho ante las autoridades competentes.

COPIA CONTROLADA

- Informar de inmediato al Proceso de Gestión de Tecnologías y la Información y al líder de proceso.
- Intentar rastrear el dispositivo utilizando las funciones de geolocalización disponibles.
- Cerrar sesiones abiertas y cambiar contraseñas de las aplicaciones corporativas.
- Solicitar la desactivación del dispositivo en caso de no recuperarlo, para impedir el acceso no autorizado.

8.6.6. Virtualización de aplicaciones

La **virtualización de aplicaciones** permite ejecutar software corporativo sin instalarlo directamente en el equipo personal.

Su uso:

- Reduce riesgos de seguridad, ya que el sistema operativo local no se modifica.
- Facilita la disponibilidad permanente de las herramientas institucionales.
- Permite un control centralizado de actualizaciones y configuraciones.

8.6.7. Resguardo de documentos

Los documentos y archivos laborales deberán almacenarse en repositorios corporativos seguros, preferiblemente en la nube institucional (OneDrive empresarial) y no en el equipo personal.

Se deberán aplicar medidas de seguridad adicionales como:

- Uso de contraseñas robustas.
- Activación de la **verificación en dos pasos (2FA)**.
- Respaldo periódico de la información crítica.

COPIA CONTROLADA

8.6.8. Bloqueo de dispositivos

- Durante el teletrabajo, el usuario deberá **bloquear la pantalla** de su equipo cada vez que se ausente, incluso si se encuentra en su domicilio.
- El computador debe contar con contraseña de inicio de sesión.
- Esta práctica evita accesos accidentales o intencionales a la información institucional por parte de terceros.

8.6.9. Uso de servicios corporativos

Los funcionarios deberán utilizar exclusivamente los servicios y plataformas institucionales para el intercambio y almacenamiento de información, tales como OneDrive, SharePoint y correo corporativo.

Está prohibido utilizar servicios personales como Google Drive, Dropbox u otros no aprobados.

La entidad no se hace responsable de la seguridad ni de la configuración de cuentas personales o dispositivos ajenos al entorno corporativo.

8.6.10. Vigilancia ante posibles amenazas

El teletrabajo incrementa la cantidad de comunicaciones digitales, por lo que los usuarios deberán estar alertas frente a correos o mensajes sospechosos.

Se recomienda:

- Verificar la autenticidad del remitente antes de responder o abrir enlaces.
- Desconfiar de solicitudes urgentes de pagos o entrega de información.

COPIA CONTROLADA

- Acceder directamente a las plataformas institucionales escribiendo la dirección en el navegador, sin seguir enlaces externos.
- Reportar cualquier intento de phishing o correo malicioso al Proceso de Gestión de Tecnologías y la Información.

8.6.11. Acceso mediante software remoto

Para la conexión remota entre el equipo personal y los equipos corporativos, sólo podrán utilizarse herramientas autorizadas por la entidad, con las configuraciones de seguridad adecuadas.

8.6.11.1. HopToDesk

Es una herramienta gratuita y de código abierto para control remoto, que permite cifrado de extremo a extremo.

Deberá configurarse correctamente antes de su uso, garantizando la protección de la conexión.

8.6.11.2. Configuración

El software debe instalarse en ambos equipos (local y remoto), cada uno con su propio ID y contraseña. La comunicación permite opciones de chat, modo pantalla, transferencia de archivos y activación del modo de privacidad.

8.6.11.3. Funciones de escritorio remoto

HopToDesk admite el acceso desatendido; sin embargo, esta función deberá mantenerse desactivada por defecto, salvo que se configure con una contraseña permanente y segura.

COPIA CONTROLADA

8.6.11.4. Autenticación

Si se sospecha que la contraseña de acceso ha sido comprometida, se deberá regenerar de inmediato. Las contraseñas permanentes deberán cambiarse periódicamente.

8.6.11.5. Modo privacidad

El modo privacidad oculta la actividad del equipo remoto durante la sesión, evitando la visualización no autorizada.

8.6.11.6. Lista de dispositivos

HopToDesk clasifica los equipos conectados en tres apartados: Sesiones recientes, Favoritos y Descubiertos, permitiendo una mejor gestión de conexiones seguras.

8.6.11.7. Permisos

El usuario decidirá qué permisos concede al equipo remoto, tales como:

- Control de teclado y ratón.
- Copiar y pegar (portapapeles).
- Transferencia de archivos.

8.6.12. Autorizaciones para efectuar teletrabajo

Ningún funcionario podrá acceder a los equipos o sistemas de información empresariales sin la debida autorización formal.

COPIA CONTROLADA

8.6.12.1. Subgerencia Administrativa y Financiera

Corresponde a esta dependencia autorizar mediante documento al Proceso de Gestión de Tecnologías y la Información la utilización de conexiones remotas a los sistemas institucionales.

8.6.12.2. Proceso de Gestión de Tecnologías y la Información

Le corresponde:

- Diligenciar con el usuario los documentos requeridos.
- Verificar que el equipo cumpla con las normas mínimas de seguridad informática.
- Formalizar y firmar los acuerdos de confidencialidad correspondientes.

8.6.12.3. Accesos no autorizados

El Proceso de Gestión de Tecnologías y la Información deberá documentar los accesos no autorizados y notificar a la Subgerencia Administrativa y Financiera y/o al Área Jurídica, para la aplicación de las medidas disciplinarias pertinentes.

8.6.13. Red Privada Virtual – VPN Una Red Privada Virtual (VPN)

Es una herramienta diseñada para proteger la privacidad y permitir la conexión remota segura a la plataforma tecnológica de la Red de Salud del Centro.

Cuando un equipo se conecta mediante VPN, pasa a formar parte de la red interna institucional, por lo que debe cumplir los mismos estándares de seguridad que los equipos conectados físicamente.

COPIA CONTROLADA

Los equipos con acceso VPN deberán contar con:

- Antivirus y antimalware actualizados.
- Configuración validada por el Proceso de Gestión de Tecnologías y la Información.
- Cumplimiento de horarios y condiciones de uso establecidos (horarios limitados o 7x24 según autorización).

La creación, configuración y administración de las VPNs será competencia exclusiva del Proceso de Gestión de Tecnologías y la Información.

8.7. MEDIOS DE COMUNICACIÓN EMPRESARIALES – GESTIÓN DE LA INFORMACIÓN

Los medios de comunicación institucional son herramientas oficiales provistas por la Red de Salud del Centro para el desarrollo de actividades laborales. Su uso debe ceñirse estrictamente a fines corporativos, garantizando la confidencialidad, integridad y disponibilidad de la información transmitida a través de ellos.

8.7.1. Telefonía IP

La telefonía IP, disponible mediante terminales físicos o clientes virtuales, permite la comunicación interna a través de extensiones y la externa hacia números fijos y móviles. Las llamadas a teléfonos móviles requerirán autorización previa de la Subgerencia Administrativa y Financiera.

COPIA CONTROLADA

Este medio de comunicación deberá utilizarse exclusivamente para el cumplimiento de funciones laborales. Queda prohibido su uso con fines personales o ajenos a la misión institucional.

8.7.2. Correo institucional y almacenamiento en red (OneDrive)

El correo electrónico institucional bajo el dominio **@saludcentro.gov.co** es la única plataforma autorizada para el envío y recepción de comunicaciones electrónicas internas y externas.

La Subgerencia Administrativa y Financiera podrá autorizar temporalmente el uso de otras plataformas, con la condición de que la migración a la plataforma institucional se efectúe en un plazo máximo de 180 días calendario.

Toda información perteneciente a la Red de Salud del Centro que requiera almacenamiento externo deberá alojarse exclusivamente en repositorios corporativos bajo el dominio @saludcentro.gov.co.

Está estrictamente prohibido almacenar información institucional en servicios de terceros.
La información contenida en los repositorios institucionales solo podrá compartirse con fines laborales y no deberá sincronizarse ni descargarse en equipos de cómputos personales o no autorizados.

Nota: Queda **prohibido el uso de cuentas de correo personales** para el envío o recepción de comunicaciones laborales, tanto internas como externas.

COPIA CONTROLADA

No se otorgarán permisos excepcionales para el uso de dichos correos.

8.7.3. Mensajería instantánea

La Red de Salud del Centro autoriza el uso de las aplicaciones de mensajería **WhatsApp** y **Telegram**, conforme a la legislación colombiana vigente y a las políticas internas de seguridad informática.

El uso de estas aplicaciones durante la jornada laboral se permitirá únicamente para fines institucionales y desde dispositivos móviles corporativos o personales.

El uso de sus versiones web o de escritorio está prohibido, salvo autorización expresa del Proceso de Gestión de Tecnologías y la Información.

8.7.3.1. Objetivo de los grupos de mensajería

Los grupos de mensajería instantánea deberán crearse con un propósito laboral específico. Cada integrante deberá respetar dicho objetivo y abstenerse de enviar mensajes, archivos o enlaces ajenos a la finalidad del grupo.

8.7.3.2. Contenido de los mensajes

Los mensajes deberán redactarse de manera clara, respetuosa y profesional. Deben evitarse expresiones ambiguas, irónicas o exageradas que puedan prestarse a interpretaciones erróneas o malentendidos. El tono de comunicación debe reflejar los valores institucionales y la cultura organizacional de la Red de Salud del Centro.

COPIA CONTROLADA

8.7.3.3. Grupo de soporte de Gestión de Tecnologías y la Información

El grupo de soporte técnico del **Proceso de Gestión de Tecnologías y la Información** en la plataforma **Telegram** tiene como objetivo brindar atención inmediata a incidentes o fallas que afecten de manera significativa el desarrollo de las actividades laborales.

Las solicitudes de soporte que no sean urgentes o que presenten baja afectación deberán tramitarse a través de la plataforma de gestión de tickets **RING**, descrita en el ítem 8.7.3.4. Antes de enviar una solicitud, el usuario deberá verificar que la falla efectivamente requiera intervención técnica, con el fin de evitar reportes innecesarios o "falsos positivos".

8.7.3.3.1. Requisitos de la solicitud de soporte Toda solicitud enviada al grupo de soporte deberá contener información completa y precisa que permita brindar atención oportuna. Los datos mínimos requeridos son:

a) Descripción clara y concisa de la falla.
b) Preferiblemente incluir imagen.
c) IPS y área donde se encuentra el equipo afectado.
d) Dirección IP y/o credenciales de acceso al equipo, si aplica.

Se recomienda condensar la información en un único mensaje estructurado, evitando fragmentarla en múltiples envíos.

Se recomienda hacer las verificaciones previas de usuario, verificar que el dispositivo esté conectado a la energía, uno o más cables desconectados, etc., para evitar "falsos positivos"

COPIA CONTROLADA

En caso de que la falla se resuelva sin intervención del grupo de soporte, el usuario deberá informar su solución por el mismo canal.

8.7.3.4. Plataforma de solicitudes RING (Tickets)

La **plataforma RING** (http://ring.saludcentro.gov.co/) es el sistema institucional para la gestión de solicitudes y reportes relacionados con la infraestructura tecnológica (equipos de cómputo, comunicaciones, redes, software y sistemas de información).

Su objetivo es canalizar y dar seguimiento a requerimientos no urgentes, que no comprometan de forma inmediata el desempeño de las actividades laborales.

Las solicitudes de adquisición de tecnología no se tramitan por RING; deben realizarse mediante correo institucional dirigido al líder del Proceso de Gestión de Tecnologías y la Información.

8.7.3.4.1. Contenido del ticket Cada caso reportado en la plataforma RING deberá contener los siguientes datos obligatorios:

a) Descripción detallada del inconveniente o solicitud.
b) IPS donde se ubica el equipo afectado o donde se propone la solución.
c) Área o dependencia correspondiente.
d) Identificación del equipo: número de activo fijo, dirección IP o extensión telefónica.
e) Nombre completo del solicitante.
f) Teléfono de contacto.

COPIA CONTROLADA

Cada ticket debe corresponder a un único caso.

En lo posible, la solicitud deberá ser registrada por la persona directamente afectada. Si la gestión la realiza un tercero, deberá indicarse expresamente y suministrar los datos de contacto del usuario afectado.

8.8. DISPOSICIONES FINALES

- El incumplimiento de las políticas establecidas en este capítulo podrá derivar en sanciones disciplinarias conforme a la normativa institucional vigente.
- El uso responsable, ético y seguro de los medios de comunicación corporativos es **obligación de todos los funcionarios y contratistas** de la Red de Salud del Centro.
- El Proceso de Gestión de Tecnologías y la Información podrá auditar y monitorear el uso de los medios electrónicos con el fin de garantizar la seguridad de la información y el cumplimiento de las políticas aquí descritas.

9. ENFOQUE DIFERENCIAL

La implementación del enfoque diferencial a través de este manual no solo garantiza la accesibilidad digital mediante herramientas como lengua de señas en la página web, ampliación del tamaño de letra, contrastes adaptativos y lectores de pantalla, sino que también asegura que estas soluciones cumplan con los estándares de seguridad informática. Cada

COPIA CONTROLADA

recurso inclusivo debe estar protegido contra vulnerabilidades, evitando riesgos como accesos no autorizados, alteración de contenidos o fuga de información sensible. Asimismo, se establecen protocolos para que las adaptaciones tecnológicas (por ejemplo, plugins de accesibilidad o sistemas de interpretación) sean validadas por el Proceso de Gestión de Tecnologías y la Información, asegurando que la inclusión y la protección de datos trabajen de manera conjunta para ofrecer un servicio seguro, equitativo y confiable.

TROLADA

10. ANEXOS

Aplicativo para el reporte de novedades asociadas a Software y Hardware

11. DOCUMENTOS RELACIONADOS

Interno / Externo	Nombre	Código / Ubicación
Interno	Procedimiento para el manejo de pérdida por daño, hurto o extravío de activos	GAF-P-018
Interno	Reporte de pérdida por daño, hurto o extravío de activos	GAF-F-061
Interno	Solicitud de navegación abierta yo restringida por internet	GTI-F-013
Interno	Traslado de equipos de cómputo y comunicaciones	GTI-F-001
Interno	Solicitud de diagnóstico de equipo de cómputo y comunicaciones	GTI-F-008
Interno	Cronograma de mantenimiento de equipos de cómputo y comunicaciones	GTI-F-007
Interno	Manual usuario equipos de computo	GTI-M-001
Interno	Procedimiento copias de seguridad bases de datos	GTI-P-012
Interno	Procedimiento de Auditoria a equipos de cómputo	GTI-P-026
Interno	Creación (alta) y retiro (baja) de usuarios en plataformas institucionales	GTI-P-027
Interno	Política de seguridad y privacidad de la información	GTI-PO-005
Interno	Política de tratamiento de riesgos de seguridad y privacidad de la información	GTI-PO-006

COPIA CONTROLADA

12. BIBLIOGRAFÍA

- Ley 23 de 1981 – Normas sobre ética médica.
- Ley 9 de 1979 – Medidas sanitarias y control de calidad en servicios de salud.
- Ley 527 de 1999 – Comercio electrónico y firma digital (para historias clínicas electrónicas).

- Ley 1273 de 2009 – Modifica el Código Penal colombiano para tipificar delitos informáticos y proteger la integridad de los datos y sistemas.
- Ley 1581 de 2012 – Protección de datos personales.
- Ley 1751 de 2015 – Ley Estatutaria de Salud (derecho fundamental a la salud).
- Decreto 780 de 2016 – Sistema Obligatorio de Garantía de Calidad en Salud.
- Resolución 1995 de 1999 – Regula la historia clínica: debe ser única, integral, cronológica y segura. Conservación mínima: 20 años.
- Resolución 3100 de 2019 – Condiciones de habilitación de servicios de salud.
- Resolución 839 de 2017 – Seguridad del paciente y reporte de eventos adversos.
- Manual de Gobierno Digital. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), Colombia.
- ISO 27001 – Gestión de seguridad de la información (aplicable a salud). Estándar internacional para la gestión de la seguridad de la información, que establece requisitos para implementar un Sistema de Gestión de Seguridad Informática (SGSI).

COPIA CONTROLADA

CONTROL DE CAMBIOS Y REVISIONES				
Revisión	**Fecha**	**Versión anterior**	**Versión actual**	**Cambio realizado**
01	01/04/2021	01	02	Se incluyo el Teletrabajo
02	01/08/2023	02	03	Se incluyo Almera, nueva plataforma de Tickets RING, cambio del nombre del proceso adicionando TIC, restricciones de uso de memorias USB.
03	31/10/2024	03	04	Se cambio plataforma AnyDesk por HopToDesk, se cambió el nombre del proceso de Gestión de la Información a Gestión de Tecnologías y la Información, se cambió plantilla de manual
04	19/11/2025	04	05	1. Revisión y ajuste normativo en la redacción de: * 1.1 Introducción

CONTROL DE CAMBIOS Y REVISIONES				
Revisión	**Fecha**	**Versión anterior**	**Versión actual**	**Cambio realizado**
				* 1.2 Objetivo * 1.3 Alcance * 1.4 Contenido (Se garantiza alineación con políticas institucionales y estándares vigentes). 2. Eliminación de ítems no autorizados: * 2.1 Spark * 2.2 Team Viewer (En cumplimiento de lineamientos de seguridad y control de software). 3. Incorporación de nuevas restricciones: Bloqueo de navegación en modo incógnito (Medida orientada a reforzar la trazabilidad y la protección de datos). 4. Ampliación de responsabilidades: Se definen roles y obligaciones adicionales para asegurar la correcta aplicación de políticas y la mitigación de riesgos.

Elaboró:	**Revisó:**	**Aprobó:**
Ing. Freddy Alberto Castillo Zabala Profesional administrativo	Ing. Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información	Dra. Angela María Calero Subgerente Administrativo y Financiero

COPIA CONTROLADA