POLITICA DE SEGURIDAD DE LA INFORMACION

E.S.E. HOSPITAL DE PUERTO COLOMBIA

YURLAY QUINTERO GOMEZ
GERENTE

Elaboró:	Revisó:	Aprobó:
Grupo MIPG	Planeación - Calidad	Dra. Yurlay Quintero Gerente –

1. Objetivo General

La declaración de **la Política de Seguridad de la Información Institucional** busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión.

La política de seguridad de la información se consolida a través de los procedimientos, guías, instructivos, publicaciones, controles tecnológicos y administrativos, así como en la asignación de roles y responsabilidades.

2. Objetivos específicos.

a) Mejorar continuamente las capacidades y habilidades necesarias en todos los servidores públicos para identificar, reportar y gestionar los riesgos de seguridad digital mediante acciones de sensibilización y capacitación

b) Implementar, mantener y mejorar anualmente el conjunto de controles de seguridad de la información recomendados por el modelo de seguridad y privacidad de la información mediante la aplicación del plan de seguridad y privacidad de la información institucional, para mantener en niveles aceptables los riesgos residuales de seguridad digital.

c) Fortalecer continuamente la función institucional mediante la implementación, difusión y mejoramiento continuo del modelo de seguridad y privacidad de la información para mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad.

3. . Alcance

Las políticas de Seguridad de la Información son aplicables a todos los servidores públicos,y contratistas de la entidad que procesan y/o manejan información de la, incluidas las operaciones de recopilación, análisis, procesamiento, disponibilidad, custodia, conservación y recuperación.

4. Generalidades

Administración de las políticas de seguridad de la información

Las políticas de seguridad de la información se revisan periódicamente con el fin de garantizar su vigencia y pertinencia para el cumplimiento de los objetivos institucionales. De la misma forma se revisan cuando se presenten situaciones como: cambios organizacionales, o del entorno interno o externo, cambios operativos o normativos que afecten a la entidad, cuando ocurren incidentes de seguridad de la información que obliguen al fortalecimiento de controles o lineamientos, o de acuerdo con los resultados de la gestión de riesgos institucionales. De igual manera, se implementan mediante lineamientos, procedimientos o controles que especifican los detalles técnicos de su operación.

5. Marco normativo

- Constitución Política de Colombia Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar”. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
- Constitución Política de Colombia Articulo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.
- Ley 23 de 1982, Sobre derechos de autor
- Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- Ley 603 de 2000, Por la cual se modifica el artículo 47 de la Ley 222 de 1995
- Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
- Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.
- Ley 734 de 2002, Por medio de la cual se expide del código único disciplinario.
- Ley 1032 de 2006, Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000.
- Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

•Ley 1221 de 2002 Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

• Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC.

• Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

• Ley 1336 de 2009 (Lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.) por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

• Ley 1437 DE 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Articulo 1 de la ley 1755 de 2015.

• LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

• Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

• Ley 1672 de 2013, Lineamientos para la Adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos

• Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

• Ley 128 de 2018, Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

• Ley 1955 del 25 de mayo de 2019. "Por el cual se expide el Plan Nacional de Desarrollo 2018- 2022. "Pacto por Colombia, Pacto por la Equidad". Incluyó el artículo 147 de Transformación Digital Pública y 148 de Gobierno Digital como política de gestión y desempeño institucional

• Decreto 1474 de 2002, por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).

A• Plan Institucional de Archivos PINAR: El PINAR se desarrolla para asegurar la articulación del PGD con la misión, objetivos y metas estratégicas del AGN.

6. Definiciones

- **Activo:** cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Activo de Información:** recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación). • Amenaza: causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la organización.
- **Amenaza informática:** situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado
- **Antivirus**: programas cuyo objetivo es detectar y eliminar software malicioso.
- **Análisis de riesgos**: proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo**.**
  - **Accesibilidad:** facilidad con que la información estadística puede ser ubicada y obtenida por los usuarios. Contempla la forma en que ésta se provee, los medios de difusión, así como la disponibilidad de los metadatos y los servicios de apoyo para su consulta.
  - **Análisis predictivo:** acción que implica proponer escenarios futuros a partir de la aplicación de diferentes métodos estadísticos de proyección, por ejemplo, de: tendencia, incremental, mínimos cuadrados, entre otros.
  - **Análisis sistémico:** comprender el comportamiento de un sistema a través de la interacción de los elementos que lo componen.
  - **Analítica de datos:** se refiere al manejo de datos con la intención de identificar patrones y/o tendencias que generen proyecciones para la toma de decisiones basada en evidencia.
  - **Arquitectura empresarial:** es una práctica estratégica que consiste en analizar integralmente la entidad desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad. Una arquitectura se descompone en varias estructuras o dimensiones para facilitar su estudio. En el caso colombiano, se plantea la realización de la arquitectura misional o de negocio y la definición de la arquitectura de TI, cuya descomposición se hizo en seis dominios: Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación.
  - **Autocontrol:** capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para

el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política.

- **Autogestión:** capacidad de toda organización pública para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada por la Constitución, la ley y sus reglamentos.
- **Barreras para la innovación:** factores internos o externos a la entidad que detienen o retrasan esfuerzos enfocados a la innovación
- **Back up**: se refiere a una copia de respaldo de información. •
- **Buzón**: espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros.
- **Canal de comunicación:** medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.
- **Centro de cómputo**: espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también data center por su término anglosajón.
- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio**: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.
- **Bases de Datos:** conjunto de resultados y la documentación que los soportan, que se obtienen de las operaciones estadísticas y que describen o expresan características sobre un elemento, fenómeno u objeto de estudio
- **Calidad:** entendida como el impulso hacia la mejora permanente de la gestión, para satisfacer cabalmente las necesidades y expectativas de la ciudadanía con justicia, equidad, objetividad y eficiencia en el uso de los recursos públicos
- **Canal itinerante:** espacios adicionales que cada entidad puede crear por un período determinado de tiempo para poner a disposición de la ciudadanía, su oferta de trámites y servicios, como, por ejemplo, las ferias de servicios.
- **Clima organizacional:** es el ambiente propio de la entidad, producido y percibido por los servidores de acuerdo a las condiciones que encuentra en su proceso de interacción social y en la estructura organizacional que se expresa por variables que orientan su creencia, percepción, grado de participación y actitud; determinando su comportamiento, satisfacción y nivel de eficiencia en el trabajo.
- **Código de Integridad:** herramienta diseñada por Función Pública en la cual se establecieron unos mínimos de integridad homogéneos como base para todos los servidores públicos del país, y para que las entidades promuevan sus propios procesos de socialización y apropiación en su cotidianidad, a través de la inclusión de principios de acción particulares sobre los 5 valores del Código General.

- **Comité Institucional de Coordinación de Control Interno:** es el órgano asesor e instancia decisoria en los asuntos de control interno de una entidad pública (Decreto 1083 de 2017, artículo 2.2.21.1.5).
- **Comité Institucional de Gestión y Desempeño:** Encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG, el cual sustituye los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal (Decreto 1499 de 2017, art 2.2.22.3.8.)
- **Direccionamiento Estratégico:** ejercicio emprendido por el equipo directivo de una entidad, en el que, a partir del propósito fundamental de la misma, las necesidades de sus grupos de valor, las prioridades de los planes de desarrollo (nacionales y territoriales) y su marco normativo, define los grandes desafíos y metas institucionales a lograr en el corto, mediano y largo plazo, así como las rutas de trabajo a emprender para hacer viable la consecución de dichos desafíos.
- **Esquema de líneas de defensa:** esquema de asignación de responsabilidades para la gestión de riesgos y del control en una entidad, a través de cuatro roles: línea estratégica, integrada por la alta dirección de la entidad y el comité institucional de control interno; primera línea de defensa, integrada por los gerentes públicos y líderes de procesos, programas y proyectos; segunda línea de defensa, integrada por las oficinas de planeación, líderes de otros sistemas de gestión o comités de riesgos; tercera línea de defensa, integrada por las oficinas de control interno. Este esquema permite distribuir estas responsabilidades en varias áreas y evitando concentrarlas exclusivamente en las oficinas de control.
- **Indicador:** Variable o factor cuantitativo o cualitativo que proporciona un medio sencillo y fiable para medir logros, reflejar los cambios vinculados con la gestión o evaluar los resultados de una entidad
- **Grupos de Interés:** Individuos u organismos específicos que tienen un interés especial en la gestión y los resultados de las organizaciones públicas. Comprende, entre otros, instancias
- **Grupos de valor**: Personas naturales (ciudadanos) o jurídicas (organizaciones públicas o privadas) a quienes van dirigidos los bienes y servicios de una entidad (Glosario, Sistema de Gestión, Modelo Integrado de Planeación y Gestión, Versión 3, pág. 5).
- **Meta:** Expresión concreta y cuantificable de los logros que la organización planea alcanzar en un periodo de tiempo, con relación a los objetivos previamente definidos (Glosario, Sistema de Gestión, Modelo Integrado de Planeación y Gestión, Versión 3, pág. 7).
- **Nivel de Satisfacción:** Medida relacionada con el grado de expectativa de los grupos de valor, en el desarrollo de las actividades, procesos o prestación de servicios en cuanto a su calidad y pertinencia (Glosario, Sistema de Gestión, Modelo Integrado de Planeación y Gestión, Versión 3, pág. 7).

- **Objetivos estratégicos:** Es la expresión de los logros que se espera que las entidades públicas alcancen en el largo y mediano plazo, en el marco del cumplimiento de su propósito fundamental y de las prioridades del gobierno (Glosario, Sistema de Gestión, Modelo Integrado de Planeación y Gestión, Versión 3, pág. 7).
- **Planeación Institucional:** es un instrumento a través del cual se realiza la planeación de las acciones orientadas a fortalecer la implementación de las políticas gestión y desempeño, basado en el resultado de la medición del FURAG, de la aplicación de las herramientas de autodiagnóstico, de las auditorías de los entes de control y de la Oficina de Control Interno, entre otras fuentes de información (Circular 1 de 2018, DAFP).
- **Política:** Directriz emitida formal por la dirección sobre lo que hay que hacer para efectuar el posterior control.
- **Promoción de la integridad:** se entiende como la manera constante y permanente de hacer las cosas incorporando hábitos, actitudes y percepciones de los servidores públicos frente a la prevención de la corrupción y la transparencia y eficiencia en la gestión.
- **Recursos presupuestales:** Son las asignaciones consignadas en el presupuesto anual de cada entidad, acorde con las normas que rigen la materia para cada una, y que le permiten definir monto de gastos a incurrir para cumplir con sus funciones y competencias, para producir los bienes y prestar los servicios a su cargo
- **Resultado:** Producto, efecto o impacto (intencional o no, positivo y/o negativo) de la gestión de una entidad pública, a partir de los bienes que genera y los servicios que presta a sus grupos de valor

7. Responsabilidad por contravención de la política de seguridad

El incumplimiento de la política de seguridad de la información descritas en este documento se trata mediante el procedimiento de incidentes de seguridad de la información, de acuerdo con la naturaleza del incidente y los resultados de su tratamiento e investigación y los responsables de los procesos institucionales evalúan la necesidad de adelantar procesos disciplinarios o legales. Cuando los incidentes de seguridad de la información correspondan a delitos informáticos calificados como tales por la normatividad vigente, se formulará la recomendación al Comité Institucional de Gestión y Desempeño para iniciar las acciones legales ante la respectiva autoridad competente. Cuando el incidente de seguridad de la información no esté calificado como un delito informático, las acciones disciplinarias o legales se adelantan de acuerdo con la competencia del código único disciplinario en el caso de servidores públicos o mediante los criterios definidos en los contratos de prestación de servicios en el caso de contratistas.

8. Roles y responsabilidades en materia de seguridad de la información

La política de seguridad de la información es de aplicación obligatoria para todo el personal de la entidad, cualquiera sea su calidad jurídica, el área a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñé. Todos los servidores públicos, contratistas, proveedores y cuando sea aplicable los grupos de valor, deben utilizar los activos de información institucionales para el desarrollo de las actividades misionales, nunca para su beneficio personal o en detrimento de los objetivos institucionales. De igual forma, todos los servidores públicos, contratistas y proveedores deben preservar la confidencialidad de la información que por razones de su cargo o responsabilidades designada esté bajo su custodia.

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES es responsable de:

- Administrar y custodiar los equipos de hardware y comunicaciones alojados en el centro de datos.
- Gestionar los servicios de información y de tecnología alineados con los objetivos sectoriales e institucionales para el cumplimiento de su misión.
- Custodiar la información almacenada en los sistemas de información, aplicaciones y bases de datos.
- Disponer de las medidas de seguridad para proteger la información digital de la ESE Informar al Comité Institucional de Gestión y Desempeño de los eventos de seguridad que se presenten y la solución planteada.
- Dar los lineamientos para la administración de los equipos de cómputo, dispositivos de almacenamiento externo, sistemas de información, aplicativos e infraestructura tecnológica.
- Responder por la disponibilidad de los servicios tecnológicos e informar al comité de emergencias cualquier novedad que pueda afectar la normal prestación de los mismos.
- Realizar el monitoreo y control automático del software instalado en los equipos de cómputo de la entidad. Si se encuentra instalado software no autorizado, se notificará al jefe inmediato o supervisor para que se informe el motivo de la irregularidad y se tomen las medidas del caso.

LIDER TICS. Oficial en materia de Seguridad informática . Responsabilidad .

- Aprobar las políticas de seguridad de la información.
- Evaluar el proceso de gestión de seguridad de la Información

- Definir las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité Institucional de Gestión y Desempeño.
- Facilitar los recursos requeridos para el sistema de gestión de seguridad de la información
- Organizar las actividades del Comité Institucional de Gestión y Desempeño en materia de seguridad de la información.
- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la entidad y el control de su implementación; y velar por su correcta aplicación.
- Supervisar el monitoreo del avance general de la implementación de las estrategias de control y tratamiento de riesgos de seguridad digital. ⎫
- Gestionar la coordinación con otras áreas de la entidad para apoyar los objetivos de seguridad.
- Hacer el enlace con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información.
- Apoyar a los diferentes procesos institucionales en la adopción de

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO. Responsabilidad .

- Aprobar las políticas de seguridad de la información.
- Evaluar el proceso de gestión de seguridad de la Información
- Definir las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité Institucional de Gestión y Desempeño.
- Facilitar los recursos requeridos para el sistema de gestión de seguridad de la información. Comité Institucional de Gestión y Desempeño
- Revisar y proponer al gerente , para su aprobación, la Política de Seguridad de la Información.
- Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información.
- Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas. ⎫ Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones.
- Reportar al gerente , respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución del sistema de gestión de seguridad de la información.

- Servir de enlace con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información
- Mantener contacto con las autoridades en materia de ciberseguridad para conocer de primera mano indicios o alertas en materia de seguridad de la información y recibir el apoyo de grupos de respuesta ante incidentes de seguridad de la información.
- Mantener contacto con grupos de interés especial en materia de seguridad de la información para asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa.
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades
- Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

LIDER DE TALENTO HUMANO . Responsabilidad .

- Cumplir con los procedimientos relativos al tema de Seguridad de la Información del Talento Humano.
- Notificar a todo el Talento Humano que se incorpora a la entidad, sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Ejecutar tareas de capacitación continuas en materia de seguridad de la información.
- Incorporar al Plan Institucional de Capacitación las actividades del Plan de Sensibilización en seguridad de la información, aprobadas por el Comité Institucional de Gestión y Desempeño

ASESOR JURIDICO. Responsabilidad

- Velar por el cumplimiento legal de la Política de Seguridad de la Información en la entidad.
- Definir, documentar y actualizar a solicitud del área encargada todos los requerimientos estatutarios, reguladores y contractuales relevantes en materia de seguridad de la información, y el establecer enfoque de la entidad para satisfacer esos requerimientos, para cada sistema de información y la entidad.
- Asesorar en materia legal, asociada a seguridad de la información, a la entidad y establecer las pautas legales que permitan cumplir con los requerimientos legales en esta materia

OFICINA DE CONTROL INTERNO . Responsabilidad

- Practicar auditorias periódicas, o cuando lo considere pertinente, sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.
- Informar al encargado de seguridad, el resultado de las auditorías realizadas.) Recomendar acciones de mejora frente a las debilidades encontradas en las auditorias e informarlas al Comité Institucional de Gestión y Desempeño

VISITANTES . Responsabilidad

- Cumplir las políticas de seguridad de la información institucionales cuando se les autorice acceso a los activos de información institucionales.
- Utilizar únicamente la red local de invitados, la cual restringe el acceso solo a internet.
- Solicitar al responsable del respectivo activo de información la autorización de acceso a los mismos.
- No interrumpir o deshabilitar los controles de seguridad dispuestos por la Entidad para la protección de sus activos de información.

SERVIDORES PÚBLICOS, CONTRATISTAS Y ESTUDIANTES EN PRACTICAS. Responsabilidad

- Dar buen uso de los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones o actividades, la relación de los mismos debe estar registrada en el Sistema de Inventarios de la entidad.
- Hacer entrega en buen estado de los equipos de cómputo y periféricos que le sean asignados, cuando se presente retiro de la entidad, cambio de funciones o culminación del contrato según sea el caso.
- Custodiar la información alojada en el equipo de cómputo y periféricos asignados. • Cumplir las políticas de respaldo, custodia y recuperación de la información definidas por la Oficina de Tecnologías de la Información y las Comunicaciones.
- Conectarse a la red con el usuario asignado y la respectiva clave de acceso.
- Utilizar solamente software licenciado y autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones. En caso de requerir la instalación de software

adicional, el director o jefe del área debe realizar la solicitud por medio de la Sistema de mesa de servicio, con la debida justificación para revisión y a probación.

- Permitir, cuando Función Pública lo requiera, la revisión del equipo de cómputo a nivel físico, software instalado e información alojada.

9. Uso de Internet

- La ESE , en cabeza de la Oficina de Tecnologías de la Información y las Comunicaciones dispone de un canal de Internet que apoya el cumplimiento de las funciones de los servidores públicos y pasantes.
- El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas asignadas al servidor público, contratista o parte interesada. Ver ley 734 de 2002, por la cual se expide el Código Disciplinario Único. “Artículo 34, Deberes. Numeral 4: Deberes”
- El acceso al servicio de Internet podrá ser asignado a las personas que tengan algún tipo de relación con la Entidad, ya sea como servidor público, contratista, pasante o miembro de un grupo de valor. La autorización de uso del servicio de acceso a internet para los visitantes de las instalaciones de la Entidad debe ser solicitada por los responsables de procesos o dependencias que visita la persona.
- Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña para la ESE y para los cuales este formal y expresamente autorizado.
- El acceso a servicios de redes sociales, video en línea, audio o servicios no directamente afectos a la función misional solo están autorizados a las dependencias cuya función misional requiere del servicio. La Entidad se reserva el derecho de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas a la Oficina de Tecnologías de Información y las Comunicaciones
- Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que él envíe desde las redes de datos de la ESE o se descargue desde Internet usando su cuenta de acceso

10.Prohibiciones

Para los servidores públicos, pasantes, contratistas y visitantes está prohibido:

- Intercambiar información de la ESE con terceros sin previa autorización del jefe de área, supervisor o responsable de la información.
- Instalar software no licenciad

- Descargar software no autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones. }
- El ingreso a servicios interactivos, redes sociales y servicios de mensajería instantánea para fines personales.
- Descargar e intercambiar archivos de audio, juegos, video, imágenes y software de libre distribución.
- El ingreso a páginas relacionadas con violencia, pornografía, drogas, alcohol, web proxys, hacking o cualquier sitio web que puedan implicar compromiso de seguridad de la información.
- Visitar y/o realizar transacciones a través de páginas web de entidades bancarias o comerciales

11. Uso del Correo Electrónico

- Los servidores públicos, contratistas y pasantes son responsables de todas las actividades realizadas con la cuenta de correo asignada por la entidad.
- Toda la información transmitida a través de la cuenta de correo es responsabilidad del propietario de dicha cuenta

Está prohibido:

- Suministrar los datos de acceso o clave de la cuenta de correo asignada por la entidad.
- Utilizar la cuenta de correo asignada por la entidad, para actividades personales.
- Participar en la transmisión correos spam (cadenas

12. Gestión de seguridad de la información

- La Política de Seguridad de la Información se desarrolla y actualizada en cada vigencia de acuerdo con los riesgos, los requerimientos institucionales y la normatividad colombiana, atendiendo las nuevas necesidades, la situación de la entidad y las mejores prácticas de la industria.
- El Comité de Gestión y Desempeño Institucional y el encargado de Seguridad de la Información Institucional:

i) Identifican las situaciones que serán consideradas como emergencia o desastre para la ESE

ii) definen las actuaciones ante la presencia de incidentes de seguridad y desastres

iii) coordinan los temas relacionados con la continuidad del negocio y la recuperación ante cualquier tipo de desastre,

iv) aseguran la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y documentando el resultado de dichas pruebas.

- Garantiza que los planes de contingencia incluyan las consideraciones de seguridad de la información necesaria y requerida, para el cumplimiento de los objetivos trazados.

13. Control de cambios

Versión	Descripción	Vigencia
01	Elaboración del documento	2025