POLITICAS EMPRESA DE SERVICIOS PÚBLICOS DE SABANETA E.S.P – EAPSA

GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

EMPRESA DE SERVICIOS PÚBLICOS DE SABANETA E.S.P – EAPSA

ENERO 2025

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La información es un activo de alto valor para la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA a medida que los procesos de la entidad se hacen más dependientes de la información y de la tecnología que la soporta, es necesario, generar lineamientos y normas que permitan el control y administración efectiva de los datos.
Con el desarrollo avanzado de la tecnología y la dependencia de las herramientas para el desarrollo de las actividades en la organización; se incrementa la vulnerabilidad y el riesgo que afecta la seguridad de los servicios de las TICS, como:

- Ataques a través de software malicioso o virus informáticos.
- Ataque de intrusión.
- Ingreso de correos no deseado con contenido malicioso (correo fraudulento).
- Uso de claves de acceso a la red sin la consciencia de su confidencialidad.
- Instalación de software no institucional y/o no licenciado.
- Pérdida de información crítica de la entidad.
- Manejo de memorias USB con información confidencial o critica de la entidad.
- Accidente o desastre que interrumpa o degrade los servicios.
- Mal uso de los privilegios de acceso a la información o entrega de información confidencial de manera accidental o deliberada.
- El no uso del servidor corporativo para almacenar y proteger la información que comprenda el desarrollo del cargo.

El presente manual contiene los lineamientos que rigen el uso y apropiación de la información en formato físico o digital tanto para los usuarios internos como para contratistas externos o proveedores, en cumplimiento de las disposiciones legales vigentes, con el objeto de minimizar los riesgos y salvaguardar la información de la entidad.

PROPÓSITO

Proporcionar a los funcionarios, contratistas y usuarios de la Entidad un instrumento orientador para asegurar la información y el adecuado manejo de las TI, minimizando los riesgos en los que puede estar expuesta la información a fin de mantener su disponibilidad, integridad y confidencialidad y el uso de las TIC de manera eficaz, eficiente y uniforme.

PRINCIPIOS

Las políticas contenidas en el presente manual se justifican y sustentan en los principios de la seguridad de la información, tales principios son:

- Propuesta de explicar el detalle de cada principio.
- Promover comportamientos de seguridad responsables.
- Exhortar las actuaciones profesionales y técnicas.
- Promover una cultura positiva para la seguridad.
- Tener un enfoque basado en los riesgos.
- Buscar el cumplimiento de los requisitos legales y regulatorios pertinentes.
- Promover la mejora continua.
- Proteger la información clasificada.
- Evaluar las amenazas actuales y futuras de la información.
- Proteger la organización.
- Soportar el actuar de la entidad.
- Enfocarse en la organización.
- Ofrecer calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad.
- Concentrarse en aplicaciones organizacionales críticas.
- Buscar el desarrollo de sistemas de información de forma segura.

ROLES Y RESPONSABILIDADES ASOCIADAS A LA PRESENTE POLÍTICA

Comité de Dirección de Seguridad de la Información.

La entidad reglamentará su creación, sus funciones son:

- Formular y mantener actualizadas las políticas de seguridad de la información para toda la entidad.
- Revisar, aprobar y promover el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

Asesores, gerente, directores y profesionales con personal a cargo.

- Asegurar que los servidores públicos y contratistas bajo su responsabilidad conozcan, entiendan y atiendan las políticas contenidas en el presente manual.

- Aplicar controles o medidas que garanticen el cumplimiento de las políticas de seguridad de la información dentro de los procesos del Sistema Integrado de Gestión que lideren.

Servidores públicos y contratistas externos.

- Conocer y cumplir las políticas indicadas en este manual.
- Reportar las infracciones o incumplimientos que identifique.
- Apoyar a otros servidores en el cumplimiento de las políticas indicadas en este manual

Oficial de seguridad de la información.

- Dirigir el plan estratégico de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de las políticas definidas y aprobadas por el Comité de Dirección de Seguridad de la Información.
- Identificar oportunidades para la mejora de las políticas de seguridad de la información en función de las necesidades de la entidad y de los riesgos que sean identificados.
- Cumplimiento de requisitos legales y regulatorios.

Las políticas de seguridad de la información fueron definidas de conformidad a lo establecido en:

- Ley 1712 de 2014. Ley de transparencia y del derecho de acceso a la información pública nacional.
- Ley 1581 de 2012 y decreto 1377 de 2013. Ley de protección de datos personales.
- Ley 1273. Ley de delitos informáticos y la protección de la información y de los datos.
- Decreto 2693 DE 2012. Lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia.
- Decreto 1078 del 26 de mayo de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 527/1999. Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

PROCESO DISCIPLINARIO Y SANCIONES

El desacato o incumplimiento a las presentes políticas por parte de un servidor público o contratista de la Empresa de Servicios Públicos de Sabaneta E.S.P puede acarrear sanciones disciplinarias. Dichas medidas se impartirán en coherencia con la ley vigente y el reglamento interno de trabajo de la entidad.
Una infracción o falta de estas políticas por parte de un contratista externo puede generar la terminación de su contrato.

DEFINICIONES

Activo de información: Todo aquello que tiene valor para la entidad y por lo tanto debe protegerse. De acuerdo con la norma ISO 27001 los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

Borrado seguro: Procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.

Centro de Servicios Informáticos (CSI): Equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA.

Comité de Dirección de Seguridad de la Información: Equipo interdisciplinario conformado por servidores públicos de diferentes áreas la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, que es presidido por el gerente o a quien este delegue. Su función principal es la de gobernar y orientar gestión de la seguridad de la información en la empresa.

Confidencialidad: Que la información solo sea accedida por las personas autorizadas.

Contratista: Trabajador que sin tener una vinculación laboral directa con la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, presta sus servicios para la entidad (por ejemplo, a través de un contrato de prestación de servicios o por medio de una organización que tenga un contrato con la entidad).

Correo masivo: Expresión usada en el presente manual de políticas para referirse a mensajes de correo electrónico enviado a un grupo indeterminado de destinatarios que no formen parte de los dominios de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA.

Criterio de seguridad de la información: Conjunto de requisitos técnicos que deben considerarse para la planeación e implementación segura de infraestructura y aplicaciones de tecnología de información, así como para su posterior verificación.

Custodio de la información: Usuario de la información que ejerza funciones de administración de sistemas de información. Sus responsabilidades son:

- Garantizar que se cumplan los niveles de servicio definidos.
- Proporcionar asistencia al dueño de la información en la selección de soluciones técnicas apropiadas.
- Proveer operativamente el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

Derechos / Privilegios de acceso: Conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso (repositorio información, aplicativo, datos).

Disponibilidad: La información estará lista para acceder a ella o utilizarse cuando se necesite.

Dispositivos móviles: Aparatos con algunas capacidades de procesamiento y de conectividad. Su principal característica es su movilidad. Los dispositivos móviles abarcan una gran variedad de equipos como: teléfonos inteligentes, asistentes digitales personales (PDA), tabletas, y computadoras portátiles.

Dueño de activo de información: (o propietario): Servidor público de nivel directivo cuyo rol implica entender qué tipo de información es mantenida, creada, procesada o eliminada; cómo la información se desplaza en su área de responsabilidad y quien debe acceder a la información y por qué. Como resultado, son capaces de entender e identificar los riesgos a la información.
Tiene la responsabilidad de asegurar la clasificación de los activos y tomar decisiones sobre estos (por ejemplo: ubicación, acceso y controles de seguridad).

Entidad: Término que se usa en el presente documento para identificar a la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA cuando sea conveniente.

Equipos de trabajo de informática: Equipos de trabajo de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, que son responsables de desarrollar, desplegar, mantener, proteger y administrar las plataformas de tecnología de información. Abarca a los integrantes de la Líder del Proceso de Gestión de la Información y Comunicación y personal de otras áreas de la entidad con alguna de las responsabilidades mencionadas.

Equipo de seguridad de la información: Grupo funcional adscrito al Líder del Proceso de Gestión de la Información y Comunicación, cuya función primordial es la de gestionar la seguridad de la información para el alcance previsto del Sistema de Gestión de seguridad de la Información SGSI de la entidad, buscando que el nivel de riesgo de la información de la entidad permanezca en niveles aceptables.

Evento de seguridad de la información: Presencia identificada del estado de un sistema, servicio o red, que indica una posible violación de las políticas de seguridad de la información, una falla de los controles, o una situación desconocida previamente que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Todo incidente es un evento, más no todo evento es un incidente.

Integridad: La información debe estar completa y correcta en todo momento.

Seguridad informática: Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.

Servidores Públicos: Término que se usa en el presente documento para identificar a empleados públicos, trabajadores oficiales y practicantes de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA.

Sistema de Gestión de Seguridad de la Información - SGSI: Sistema de gestión basado en un enfoque hacia los riesgos, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
El SGSI se rige por los requisitos de la norma internacional de gestión ISO/IEC 27001.

Software malicioso: También conocido como código malicioso, es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario.
El software malicioso incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo y crimeware. El término “software malicioso” también hace referencia a software hostil o molesto.

Usuario: Persona, proceso o aplicación de la entidad autorizada para acceder a la información de entidad o a los sistemas que la manejan.

Zonas restringidas de procesamiento: Son áreas, recintos o edificaciones ubicadas dentro de las sedes de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, destinadas a alojar las plataformas de tecnología de la información, recursos importantes o información de la entidad; razón por la que requieren controles especiales de seguridad física y control de acceso.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo estratégico para las operaciones diarias de la Empresa de Servicios Públicos de Sabaneta E.S.P y a su vez un factor determinante para el éxito de su plan de desarrollo.

Por ello, la entidad está comprometida con la adopción de buenas prácticas de seguridad de la información tendientes a implementar, mantener y mejorar su Sistema de Gestión de Seguridad de la Información SGSI.

Las Políticas y lineamientos de Seguridad de la Información y de las TI son de carácter obligatorio y deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos que hagan uso de la información y de los recursos tecnológicos de la entidad.

1. POLÍTICAS PARA SERVIDORES PÚBLICOS Y CONTRATISTAS

Estas políticas aplican tanto a los procesos realizados directamente por la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, como a los ejecutados a través de contratos o acuerdos con terceros.

Deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos de la entidad y de las sedes externas de la entidad que hagan uso de la información institucional y de sus recursos tecnológicos.

Comprende desde la explicación de los riesgos a los que están expuestos los activos de información, hasta la ejecución y seguimiento al cumplimiento de las normas y/o políticas informáticas.

Las políticas de seguridad de la información también aplican para los servidores públicos en modalidad de teletrabajo.

2. POLÍTICAS DE IDENTIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información SGSI de la Empresa de Servicios Públicos de Sabaneta E.S.P -

EAPSA deben ser identificados, clasificados y definidos por los responsables de cada uno de ellos. Se busca asegurar que la información recibe el nivel de protección apropiado de acuerdo con la clasificación establecida.

Identificación y clasificación de la información.

- Los activos de información deben ser identificados y registrados en un inventario.
- Los activos de información deben tener propietario designado.
- El Propietario de un activo de información es responsable de:
- Definir los usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso.
- Determinar las clasificaciones correspondientes a la sensibilidad del activo.
- Asegurarse que se gestione el riesgo de seguridad del activo.
- Establecer las reglas de uso del activo, cuando sea necesario.
- Solicitar la aplicación de controles para la protección del activo de información.
- Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.

La información de la Empresa de Servicios Públicos de Sabaneta E.S.P se clasifica en:

Información pública: Es toda información que la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA genere, obtenga, adquiera, o controle en su calidad de obligado.

Información clasificada: Es aquella información que estando en poder o custodia de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA en su calidad de obligado, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

Información reservada: Es aquella información que estando en poder o custodia de la Empresa de Servicios Públicos de Sabaneta E.S.P en su calidad de obligado, es exceptuada de acceso a la ciudadanía por daño a

intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

- El manejo de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P debe seguir los lineamientos del Manual de Protección de la Información.
- Sólo se permite la transferencia de información Clasificada o Reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.
- La Empresa de Servicios Públicos de Sabaneta E.S.P tiene control total sobre la información que se almacene en la infraestructura de tecnología de la información de la entidad; por lo tanto, se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información, para lo cual deberá contar con la aprobación del director de Informática, del líder de proceso del tema en referencia y del Oficial de Seguridad.
- Los servidores públicos y contratistas son responsables de proteger la información de su trabajo y solicitar a la Líder del Proceso de Gestión de la Información y Comunicación el almacenamiento seguro de la información cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la entidad.

3. POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

En la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información, también se busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

Lineamientos generales de la gestión del riesgo de seguridad informática.

Servidores públicos y contratistas de la Empresa de Servicios Públicos de Sabaneta E.S.P, deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

Administración de Riesgos Asociados al Tratamiento de Datos.

La Empresa de Servicios Públicos de Sabaneta E.S.P. -EAPSA, ha identificado riesgos relacionados con el tratamiento de datos personales y ha establecido controles con el fin de mitigar sus causas, mediante la implementación de las políticas internas de seguridad. Por ello, estableció un sistema de gestión de riesgos junto con las herramientas y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de bases de datos y tipos de datos personales tratados por la Sociedad se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra los derechos de los Titulares.

El Oficial de Seguridad de la Información o responsable determinado caracteriza las fuentes de riesgo tales como: tecnología, recursos humanos, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo; por lo que, para garantizar la protección de datos personales se tiene en cuenta el tipo de grupo de personas internas y externas, y los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda producir un daño (material o inmaterial), tales como:

- **Criminalidad:** entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por esta.
- **Sucesos de origen físico:** Entendidos como los eventos naturales y técnicos, así como los eventos indirectamente causados por la intervención humana.
- **Negligencia y Decisiones Institucionales:** Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles ya que están directamente relacionadas con el comportamiento humano.

La organización implementará medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

Gestión de Riesgos

Bases de datos físicas: las medidas de seguridad de estas bases implican las siguientes acciones:

- Los documentos se almacenarán en armarios o archivos los cuales contarán con protectores plásticos que eviten la humedad.
- Los armarios o archivos estarán cerrados con llave, cuyas copias las deberán tener el encargado interno y el Representante legal.
- El lugar donde se encuentren los armarios estará vigilado por cámaras de seguridad 24 horas.
- El Acceso a dicho lugar solo podrá ser durante el horario laboral de la Empresa.

En el caso de que la información se almacene adicionalmente de manera digital, se tendrán todas las medidas necesarias o pertinentes para la protección de los datos y la información que se conserve de tal manera, según los lineamientos establecidos en la ley.

4. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad, con esto se busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia (confirmada o sospechada) de situaciones que afecten la seguridad de la información.

Reporte de eventos, incidentes y debilidades de la seguridad informática.

- Los servidores públicos y contratistas deben reportar inmediatamente al Centro de Servicios de Informática (CSI), todas las situaciones de las que tengan conocimiento que puedan afectar la seguridad, disponibilidad, fiabilidad o integridad de la información, describiendo detalladamente el tipo de incidente producido, las personas involucradas, los efectos que se han producido o que puedan llegar a producirse, las medidas de seguridad vulneradas o fallidas y un informe detallado de toda la información pertinente.
- La información específica sobre Incidentes o vulnerabilidades de seguridad de la información, así como el detalle de las medidas para proteger las plataformas de TIC., debe ser tratada como información reservada.

5. POLÍTICA DE USO ADECUADO DE LOS RECURSOS DE LA PLATAFORMA DE TI

Toda la información de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, así como los recursos para su procesamiento, almacenamiento y transmisión, deben ser empleados únicamente para propósitos laborales o de la entidad; evitando su abuso, derroche, uso ilegal o desaprovechamiento. Para esto se definen las directrices para asegurar el debido uso de los recursos de tecnologías de información y la comunicación de la entidad.

Requerimientos generales para el uso adecuado de la plataforma de TI.

- Se prohíbe el uso de los recursos de plataforma de TI. de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA para la realización de cualquier actividad ilegal.
- Para verificar el cumplimiento de las presentes políticas; la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA podrá monitorear y auditar las plataformas TIC de la entidad que son facilitadas a servidores públicos y contratistas para el cumplimiento de sus deberes y funciones laborales.
- Los servidores públicos y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.
- Está prohibida la realización de pruebas a los controles de seguridad de la información.
- No está permitido aprovechar las vulnerabilidades de seguridad de la plataforma de TI.
- Solamente el grupo de Seguridad de la Información o un tercero autorizado por la Líder del Proceso de Gestión de la Información y Comunicación puede
- utilizar herramientas de diagnóstico de la seguridad de la información (herramientas de hacking) sobre los activos de información de la Entidad.
- Los programas informáticos desarrollados o adquiridos por Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA son para el uso exclusivo de la entidad.

Uso adecuado del correo electrónico.

- No está permitido enviar correos masivos sin la autorización del personal directivo de la dependencia.
- La Líder del Proceso de Gestión de la Información y Comunicación podrá establecer los límites en la cantidad de destinatarios y el tamaño de los mensajes de correo electrónico.
- No está autorizado el envío de correos electrónicos con contenido que atente contra la integridad y la dignidad de las personas, así como con el buen nombre de la entidad.
- Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico se retire de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, su cuenta de correo será desactivada.
- Las cuentas de correo electrónico son propiedad de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, son asignadas para la realización tareas propias de las funciones laborales y no deben utilizarse para ningún otro fin.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.
- Cuando se detecte un correo fraudulento, con fines maliciosos o con contenido sospechoso se debe informar esta situación al Grupo de seguridad de la Información o a la mesa de ayuda del Centro de Servicios Informáticos (CSI).

Uso adecuado de equipos de cómputo asignados.

- No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.
- Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática.

Uso adecuado de los servicios de red.

- No deben almacenarse archivos personales en carpetas de la red y demás servicios de almacenamiento en internet suministrados por la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA.

- No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person). Por ejemplo: Torrent, Ares, eMule, Limewire, GNUnet, entre otros.
- No está permitida la descarga de archivos de audio y/o video a menos que lo requieran en virtud de sus responsabilidades laborales.
- La Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA podrá controlar y limitar la navegación a ciertos sitios, recursos o servicios de internet con el fin de proteger la seguridad y la disponibilidad del servicio de internet.
- No está permitido deshabilitar o evadir los controles de navegación en internet.
- En horarios laborales, está prohibido el uso del servicio de internet de la entidad para acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos.
- El acceso remoto a los equipos y dispositivos de la plataforma de TI. solo está permitido para labores de soporte técnico autorizado.
- El acceso remoto a equipos de cómputo debe contar con la aprobación del servidor público o contratista responsable de dicho equipo.
- Solo se permite el acceso remoto a estaciones de trabajo de la entidad si el servidor público o contratista responsable del equipo de cómputo lo aprueba.
- Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.
- La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente la Empresa de Servicios Públicos de Sabaneta E.S.P.
- Solo equipos matriculados en el directorio activo institucional pueden ser ingresados a la red de la Empresa de Servicios Públicos de Sabaneta E.S.P.
- No se permite la inclusión de equipos de cómputo personales (tales como PCs, computadores portátiles, celulares, tabletas, impresoras, cámaras entre otros) en la red corporativa.
- Todo equipo Tecnológico debe ser revisado, registrado y aprobado por el líder del proceso de gestión de la información y comunicación, antes de conectarse a cualquier nodo de la Red de corporativa. Aquellos dispositivos que no estén aprobados deben ser desconectados de la red, eventos de conexión de equipos no autorizados a la red institucional se deben reportar como eventos/incidentes de seguridad.

Uso de material protegido por derechos de autor.

- Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole

las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red y demás servicios de almacenamiento en internet suministrados por la entidad.

- Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) y/o licenciamiento en la plataforma tecnológica de la entidad.

6. POLÍTICA DE PERSONAS Y CULTURA FRENTE A LA SEGURIDAD INFORMÁTICA

Se deben aplicar medidas de control antes, durante y después de finalizada la relación laboral, con el fin de mitigar los riesgos de seguridad de la información asociados al factor humano.
Procura que los servidores públicos y contratistas, entiendan sus responsabilidades y las funciones de sus roles como usuarios de la información con el fin de reducir el riesgo de hurto, fraude o filtraciones.

Antes del empleo.

- Toda persona para contratar como servidor público, debe aceptar formalmente el cumplimiento de las políticas del presente manual.

Durante el empleo o la vigencia del contrato.

- Los servidores públicos y contratistas de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA son responsables por desempeñar sus funciones cumpliendo las políticas definidas en el presente manual.
- Los servidores públicos y contratistas de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA son responsables por desempeñar sus funciones sin descuidar, ignorar o desestimar los controles de seguridad establecidos.
- Los servidores públicos y contratistas que tengan acceso a la información de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA deben participar en las actividades o iniciativas de concientización en materia de seguridad de la información a las que sea convocado.
- El incumplimiento de las políticas consignadas en el presente manual podrá generar sanciones disciplinarias.

- Las políticas de seguridad informática forman parte integral de los contratos de trabajo de los servidores públicos.

Terminación del contrato o cambio de cargo.

- Servidores públicos y contratistas que finalicen su relación laboral con la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA deben entregar a su superior inmediato o responsable, la información de la entidad que se encuentre bajo su responsabilidad y/o manejo. Debe quedar registro de lo anterior en el formato “PLAN DE ENTREGA DEL CARGO” del Sistema Integrado de Gestión.
- La información y el conocimiento desarrollado por los servidores públicos de la Empresa de Servicios Públicos de Sabaneta E.S.P durante el horario laboral y dentro de la vigencia del contrato laboral es propiedad de la entidad, por lo tanto, se prohíbe el borrado o la copia de dicha información por parte de servidores públicos y contratistas en proceso de retiro o por personal retirado.
- Ante la finalización de la relación laboral o contractual de un servidor público o contratista con la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, se deben suspender inmediatamente los permisos de acceso a la plataforma de TI. de la entidad.
- La Dirección de Personal debe informar inmediatamente a la Líder del Proceso de Gestión de la Información y Comunicación, los retiros o traslados de los servidores públicos, trabajadores oficiales y practicantes, con el fin de revocar o modificar los privilegios de acceso asignados a dicho personal.
- El superior inmediato de servidores públicos y contratistas es el responsable de gestionar el retiro o modificación de los derechos de acceso ante novedades laborales como la terminación o cambio del contrato.
- El superior inmediato es el responsable de gestionar el respaldo de la información de los equipos de cómputo de los servidores públicos y contratistas en proceso de retiro.

7. POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de TI., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

Se pretende proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física, sean estas ambientales o que faciliten el acceso indebido a los activos de información.

Seguridad en las instalaciones.

- Fuera del horario laboral normal o cuando se alejen de sus estaciones de trabajo, los Servidores públicos y contratistas deben despejar sus pantallas, escritorios y áreas de trabajo, de tal manera que los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs), estén resguardados adecuadamente.
- Cuando un servidor público se percate de la presencia de personas sospechosas en las instalaciones de entidad, debe reportar dicha situación a la persona encargada de la seguridad de la información.
- No se deben prestar ni descuidar los elementos de identificación y acceso a las instalaciones de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, tales como, tarjetas de acceso, carnets, llaves y tokens.
- Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.
- Siempre que sea posible, las impresiones deben ser protegidas por medio de una clave de seguridad.
- Las reuniones y sesiones de videoconferencias de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA no deben ser grabadas en audio o video a menos que todos los participantes estén al tanto de dicha grabación. En el acta de la reunión debe registrarse que la sesión fue grabada.
- No está permitido fumar, ingerir alimentos o bebidas en las aulas con equipos de cómputo.

Seguridad de los equipos.

- Los servidores públicos y contratistas de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria.
- Los equipos suministrados por la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, como computadores de escritorio y dispositivos

móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de informática.

- Se debe bloquear la sesión cuando el usuario se aleje del computador.
- La salida de los computadores (de escritorio o portátiles) de la entidad debe ser autorizada por el gerente de la empresa.
- Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada inmediatamente al centro de servicios informáticos CSI.
- Los equipos de cómputo externos (no entregados por la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA) no deben conectarse a la red de datos de la entidad, a menos que cumplan con los requisitos definidos por la Líder del Proceso de Gestión de la Información y Comunicación. (Requisitos por definir).
- Solo personal de la mesa de ayuda (Centro de Servicios Informáticos CSI) debe tener privilegios de administración sobre los equipos de cómputo.

8. POLÍTICA DE CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN

La Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA otorga el nivel de acceso necesario a la información y su plataforma de TI. para el cumplimiento de las funciones de los servidores públicos y contratistas.
Se busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas TIC. institucionales.

Gestión de acceso a usuarios.

- Los dueños de los sistemas de información deben verificar que los privilegios de acceso de los usuarios en las plataformas de tecnología de la información se han otorgado de acuerdo con la necesidad laboral legítima.
- Los privilegios de acceso otorgados a los usuarios de las plataformas de tecnología de la información deben ser autorizados por el superior inmediato.
- Los privilegios de acceso otorgados a los usuarios de las plataformas de tecnología de Información deben ser revisados al menos anualmente por los jefes inmediatos de los usuarios.
- No están permitidas las cuentas de usuarios genéricas para el ingreso a la plataforma de TI.
- Todas las cuentas de usuario son personales e intransferibles.

- Servidores públicos y contratistas de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA deben reportar a su jefe cuando tengan más derechos de acceso de los necesarios.
- A excepción de las carpetas de red, los usuarios deben abstenerse de ingresar a los servidores de la plataforma tecnológica de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA, a menos que lo requieran en virtud de sus funciones laborales (como los administradores de plataforma de TI. de la entidad).
- En la eventualidad de requerirse el ingreso a un equipo o a alguna de las cuentas de los sistemas de información de la entidad asignadas a un servidor público ausente, el jefe directo respectivo será el único autorizado para solicitar el acceso.
- Los servidores públicos y contratistas son los responsables de todas las transacciones o acciones efectuadas con su cuenta de usuario.
- Ningún servidor público, contratista deberá acceder a la red o a los servicios de TIC. de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA utilizando una cuenta de usuario diferente a la que le fue asignada.

Manejo de contraseñas.

- Los usuarios de las Plataformas de Tecnologías de la Información de la Empresa de Servicios Públicos de Sabaneta E.S.P -EAPSA deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.
- Las contraseñas de acceso a las Plataformas de Tecnologías de la Información son personales e intransferibles, cada usuario es responsable de su uso y de preservar su confidencialidad.
- El préstamo de contraseñas está prohibido bajo cualquier circunstancia, en caso de hacerlo el usuario de la información responsable de la cuenta asume las consecuencias generadas por dicha situación.
- Los usuarios de las Plataforma de TIC. tienen la responsabilidad de cambiar su contraseña (o solicitar su cambio, si es el caso) en el evento que fuese revelada o existiese alguna sospecha de ello.
- Todos los usuarios de Las Plataformas de Tecnología de Información de la entidad deben emplear contraseñas seguras, es decir, que cumplan las siguientes características:
    - 10 caracteres como mínimo: Deben incluir letras mayúsculas y minúsculas y deben incluir números.
    - Deben incluir caracteres especiales, (Por ejemplo: !@#$%&*): No deben basarse en información personal como: fechas de cumpleaños,

direcciones, números telefónicos, nombres de personas, números de documentos de identificación, nombre de la entidad, etc.

- No deben basarse en información de la entidad, es decir, no deben hacer referencia al nombre de la entidad, sus procesos, dependencias, áreas o funciones, deben buscar establecer lineamientos tendientes a la protección de la confidencialidad de la información a través de mecanismos de cifrado.

9. POLÍTICA DE DISPOSITIVOS MÓVILES

El acceso a los datos y sistemas de información de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, a través de dispositivos móviles, debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información.
Procura proteger la información institucional que se almacena en dispositivos móviles de la entidad.

Computadores portátiles.

- Los usuarios que tengan bajo su responsabilidad computadores portátiles de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA son responsables de su protección dentro y fuera de las instalaciones de la entidad.
- Los usuarios de computadores portátiles de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA deben emplear medidas de seguridad para su adecuado manejo fuera de las instalaciones de la entidad. Las medidas de protección incluyen, pero no se limitan a:
  - Llevar los computadores portátiles como equipaje de mano en viajes terrestres y aéreos. Mantener a la vista y vigilar el computador portátil en todo momento que se esté fuera de las instalaciones de la entidad o de la vivienda del servidor público.

Dispositivos móviles diferentes a computadores portátiles.

Esta sección hace referencia a dispositivos como teléfonos móviles inteligentes y tabletas.

- Los usuarios de dispositivos móviles entregados por la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA son responsables de su protección dentro y fuera de las instalaciones de la entidad.

- Los usuarios de dispositivos móviles entregados por la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA deben abstenerse de modificar las configuraciones de seguridad de dichos dispositivos.
- Los usuarios de dispositivos móviles entregados por la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA deben reportar inmediatamente el robo o pérdida de dicho dispositivo al personal de los equipos de trabajo de informática.
- No está permitido el envío de información Clasificada o Reservada a través de servicios de mensajería instantánea no institucionales
- La Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA no está obligada a prestar soporte técnico a dispositivos móviles que sean de propiedad de los usuarios o cualquier otro que no sea propiedad de la entidad.
- Los usuarios que accedan a los servicios de la plataforma de TI. (por ejemplo, al correo electrónico) a través de un dispositivo móvil propio, deben reportar inmediatamente el robo, cambio o pérdida de dicho dispositivo al centro de servicios informáticos CSI.

10. CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN

La Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA otorga el nivel de acceso a la información necesario para el cabal cumplimiento de las funciones. Busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas TIC. institucionales.

Proceso de control de acceso.

- El control de acceso es una característica indispensable para las plataformas de tecnología de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA.
- Todo proceso de control de acceso debe tener un responsable de su gestión.
- La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación, asignación, modificación y revocación del acceso.
- Cuando aplique, las medidas de control de acceso a las plataformas de tecnología de la información deben cumplir el Criterio de seguridad de la información.
- El acceso remoto a plataformas de tecnología de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA debe ser autorizado por los dueños de las plataformas respectivas.

- El acceso remoto a plataformas de tecnología de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA debe ser realizada a través de VPN u otros medios que garanticen la seguridad en la comunicación.
- Gestión de acceso a usuarios
- Las cuentas de administración de las Plataformas de tecnología de la información sólo deben ser usadas cuando sea necesario dicho privilegio.

Manejo de contraseñas.

- Los nombres de usuario y contraseñas se rigen por el criterio de seguridad de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA.
- No se permite el uso de contraseñas fijas., todos los funcionarios sin excepción deben cambiar su password según lo establecido en el criterio de seguridad de la Información.
- Las contraseñas de administración de las plataformas de tecnología de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA, podrán ser escritas en medios físicos o electrónicos únicamente si son objeto de medidas de seguridad física y/o lógica, según lo establecido en el criterio de seguridad de la información de la Empresa de Servicios Públicos de Sabaneta E.S.P - EAPSA.
- Las contraseñas de administración de las plataformas TIC. de tener un tiempo de caducidad, o en su defecto, deben ser cambiadas periódicamente. El periodo de vigencia de las contraseñas de administración de plataforma de TI. se establece en el criterio de seguridad de la Información. (A desarrollar por la entidad).

11. FUNCIONES DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

- El Oficial de Seguridad de la Información será, de acuerdo con las necesidades de la organización, el principal encargado interno del almacenamiento, verificación y seguridad de las bases de datos e información administrada por la Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA.
- Además de aquellas que le sean expresamente asignadas el Oficial de Seguridad de la Información deberá:
- Darle el tratamiento a los datos según lo establecido en la política de tratamiento de datos según la finalidad a la que serán sometidos.

- Mantener absoluta reserva sobre la información bajo su cuidado, en los términos de ley.
- Mantener el manejo de la información y el uso de fuentes electrónicas de la organización, bajo los criterios establecidos en este Manual.
- Responder o velar por el cumplimiento dentro de los términos establecidos en la Ley 1581 del 2012 y el Decreto 1377 del 2013, las peticiones interpuestas por los Titulares de los datos.
- Informar al Titular de los datos respecto del uso que se les ha dado a sus datos personales cuando esto sea solicitado.
- En caso de revocatoria de autorización para el tratamiento de los datos personales o culminación de la finalidad para la cual fueron almacenados, deberá eliminar los registros de dichos datos conforme a lo establecido en el presente Manual.
- Conservar junto con los datos personales recopilados, la autorización por parte del Titular, en caso de que esta se dé por escrito.
- No suministrar información sobre las bases de datos a ninguna persona diferente a los Titulares, sus causahabientes, sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial, o a terceros autorizados por el Titular o por la Ley.
- Vigilar el cumplimiento de presente manual.
- Informar respecto a cualquier incidente que se presente con las bases de datos almacenadas.

La Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA podrá, a su juicio, realizar auditorías o seguimientos, con el fin de validar el cumplimiento de lo dispuesto en el presente Manual.

Cordialmente,

JUAN PABLO ARROYAVE ROMAN
Gerente
Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA