

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 1 de 35

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 2 de 35

CONTENIDO

INTRODUCCIÓN	3
GLOSARIO	4
RESUMEN	6
<i>OBJETIVO GENERAL</i>	7
<i>OBJETIVOS ESPECÍFICOS</i>	7
APLICACIÓN DE LA POLÍTICA Y RESPONSABILIDADES	8
VIOLACIONES Y SANCIONES	8
POLITICA GENERAL	9
LINEAMIENTOS OPERACIONALES O ESPECÍFICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	10
POLÍTICA DE ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO	11
POLÍTICAS DE SEGURIDAD	12
POLÍTICA PARA EL USO ADECUADO DE ESTACIONES DE TRABAJO	12
POLÍTICA PARA EL USO DE EQUIPOS DISPOSITIVOS MOVILES	17
POLITICA DE EQUIPOS TIPO PORTATIL	17
POLÍTICA PARA LA SEGURIDAD DE EQUIPOS DE PROPIEDAD DE CONTRATISTAS	19
POLÍTICAS PARA EL USO DE PROYECTORES	19
POLITICAS PARA EL USO DE RECURSOS DE RED	20
POLITICA LINEAMIENTO DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL LAN)	23
POLITICA DE CONTROL DE ACCESO	23
POLÍTICA PARA USO DE SOFTWARE	25
POLÍTICA PARA EL USO DE UNIDADES DE ALMACENAMIENTO DE INFORMACIÓN	27
POLÍTICA DE COPIAS DE SEGURIDAD	29
POLITICA DE USO DE TELEFONIA IP	30
POLITICA DE USO DE CORREOS ELECTRÓNICOS	30
POLITICAS INFRAESTRUCTURA INFORMÁTICA	32
POLITICA DE SEGURIDAD DE LOS EQUIPOS	33

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 3 de 35

INTRODUCCIÓN

Las políticas de seguridad informática son una herramienta que ayudan al funcionamiento y ejecución de las actividades que se llevan a cabo con los dispositivos informáticos en la Empresa.

Debido a cada una de las actividades que se ejecutan con los equipos informáticos que posee nuestra empresa se presentan algunas amenazas, debido al mal uso de la tecnología y de los equipos tecnológicos que se poseen, con estas amenazas se deben crear una serie de políticas que den destreza a cada uno de los usuarios y trabajadores de la empresa para que aprovechen los equipos informáticos y sus actividades de desempeño en el trabajo sean las mejores.

Con las políticas de seguridad de la EIS CÚCUTA SA E.S.P, se quiere obtener que los usuarios y empleados de la empresa, se concienticen de la buena manipulación y utilización de los recursos informáticos de la EIS CÚCUTA SA E.S.P. dándoles a conocer cada una de las medidas y precauciones preventivas que se deben tener con cada uno de los dispositivos informáticos. Igualmente, ante una dificultad puedan solucionar de forma inmediata sin la necesidad de realizar solicitud de soporte técnico al subproceso de gestión de soporte y apoyo informático.

Al implementar estas políticas se requiere que tanto los directivos como empleados tengan un gran compromiso con el cumplimiento de estas políticas.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 4 de 35

GLOSARIO

GLOSARIO	
Accidente	Es un suceso repentino no deseado que produce consecuencias negativas ya sea en las personas, las instalaciones, las máquinas o el proceso.
Activo	Cualquier cosa que tenga valor para la Empresa.
Amenaza	Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la Empresa.
Arquitectura empresarial	Conjunto de elementos organizacionales (estrategia, estructura, procesos más tecnología, personas) que se relacionan entre sí, garantizando la alineación desde los niveles más altos (estratégicos), medios (tácticos), hasta los más bajos (operativos), con el fin de optimizar la generación de productos y servicios que conforman la propuesta de valor entregada a los clientes.
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos.
Administrador	Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo un sistema informático o red de ordenadores
Ancho de banda	Máxima cantidad de datos que pueden pasar por un camino de comunicación en un momento dado, normalmente medido en segundos. Cuanto mayor sea el ancho de banda, más datos podrán circular por ella al segundo.
Computador	Es un dispositivo de computación de sobre mesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.
Contraseña	Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una Empresa autorizada

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 5 de 35

La Empresa	Se refiere a EIS Cúcuta SA E.S.P.
Dominio	El conjunto de computadoras conectadas en una red que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.
Equipo personal	Se entiende como equipo personal todo equipo perteneciente a un dueño diferente a la empresa EIS CÚCUTA SA E.S.P.
Incidente	Es un suceso repentino no deseado que ocurre por las mismas causas que se presentan los accidentes, sólo que por cuestiones del azar no desencadena lesiones en las personas, daños a la propiedad, al proceso o al ambiente.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información. Puede involucrar otras propiedades como autenticidad, trazabilidad, no repudio y fiabilidad.
TIC	Se refiere a las Tecnologías de Información y Comunicación.
Red	Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.
Servidor	Computadora que comparte recursos con otras computadoras.
Software	Todos los componentes no físicos de un PC (Programas).
Spam	Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
Usuario	Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.
Virus	Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 6 de 35

	Troya y gusano).ella a través de una red.
--	---

RESUMEN

El presente documento será de gran utilidad para cada uno de los empleados de la EIS CÚCUTA SA E.S.P. que facilite las buenas prácticas en el manejo de los equipos de cómputo, describiendo una serie de recomendaciones que podrán aportar al correcto funcionamiento de éstos, permitiendo que el trabajo no sea interrumpido por una serie de problemáticas, que pueden ser prevenidos y/o solucionadas por los mismos usuarios.

De acuerdo al análisis de la información recolectada, la observación del trabajo diario de cada una de las dependencias, grupos y subgrupos y teniendo en cuenta cada una de las problemáticas que se consideraron prioritarias para la EIS se decidió dividir las políticas en cinco grandes ítems, en donde se relaciona las precauciones que debe tener el usuario para que el funcionamiento de los equipos de trabajo y el desempeño de cada uno de los trabajadores sea el mejor.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 7 de 35

OBJETIVO GENERAL

Determinar los lineamientos que permitan garantizar que la plataforma tecnológica de la EIS CÚCUTA SA E.S.P. (recursos de software, recursos de hardware y sistemas de información) se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto, cumpliendo las normas y políticas de seguridad de la información.

OBJETIVOS ESPECÍFICOS

- ☐ Promover el uso de las mejores prácticas de seguridad informática en el trabajo, para que los usuarios colaboren con la protección de la información y recursos empresariales.
- ☐ Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con la confidencialidad, integridad y disponibilidad de la información.
- ☐ Controlar el ancho de banda, los canales de comunicación y la disponibilidad de espacio en disco en el servidor de archivos.
- ☐ Disminuir las amenazas a la seguridad de la información y los datos.
- ☐ Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
- ☐ Cuidar y proteger los recursos tecnológicos de la EIS CÚCUTA SA E.S.P.
- ☐ Concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.
- ☐ Promover las mejores prácticas de seguridad física, mediante la implementación de ambientes adecuados que permitan la correcta custodia de los datos y equipos para poder así utilizar de manera eficiente de los recursos de tecnologías de información.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 8 de 35

APLICACIÓN DE LA POLÍTICA Y RESPONSABILIDADES

La presente política deberá ser publicada en la página web de la Empresa.

Los supervisores de los distintos Procesos, Subprocesos serán responsables de ponerlas en conocimiento de su personal subordinado y demás personas de apoyo.

Para el caso del personal que se vincule o contrate con posterioridad a la fecha de publicación, se le deberá indicar el link de publicación para su conocimiento.

El encargado del subproceso de gestión de soporte y apoyo informático es el principal responsable en la definición de los criterios de seguridad de la información en la EIS CÚCUTA SA E.S.P. para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta.

Todo el personal de la Empresa tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, cualquier incidente que atente contra la seguridad de la información.

VIOLACIONES Y SANCIONES

De acuerdo al Código Disciplinario Único – Ley 734, Artículo 34, como servidor público se tiene deberes entre los cuáles se encuentran:

- Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.
- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 9 de 35

- Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

Además, en el Artículo 48, señala como falta gravísima “causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas”.

Teniendo en cuenta lo anteriormente expuesto, el incumplimiento de esta política, podrá incurrir en una falta disciplinaria. Según la gravedad que se cometa se estandariza tres niveles: leves, graves y gravísimas.

En cualquier caso, de amonestación verbal o escrita y en el caso que lo amerite, el funcionario deberá resarcir el daño o devolver, restituir o reparar el bien afectado.

Cuando se determine una falta a los deberes establecidos en la Ley 734 de 2002 y a las políticas de seguridad informática se dará a conocer a la Oficina de Jurídica y Control Disciplinario de la Institución para que en Comité determine las faltas cometidas y las sanciones a imponer de acuerdo a la norma.

POLÍTICA GENERAL

Se define la Política de Seguridad de la Información como la manifestación que hace la alta dirección de la EIS CÚCUTA SA E.S.P. sobre la intención institucional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus activos de información. La EIS CÚCUTA SA E.S.P. pretende mediante la adopción e implementación de un Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de gestión de Seguridad de la información, proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información. La EIS CÚCUTA SA E.S.P. asume el compromiso de implementar, las políticas de seguridad de alto nivel y de políticas complementarias por cada dominio de la norma ISO/IEC 27001:2013, para asegurar la confidencialidad, integridad y disponibilidad de la información.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 10 de 35

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere. La presente política debe ser revisada y actualizada anualmente o cuando el Líder de Seguridad de la Información lo determine, teniendo como criterios los cambios relevantes en el contexto interno y externo, cuando la identificación de nuevos riesgos de seguridad de la información lo requiera o cuando el marco legal que regula las políticas nacionales en materia de Seguridad de la Información, Seguridad Digital o Gobierno Digital lo demanden.

LINEAMIENTOS OPERACIONALES O ESPECÍFICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Organización de la Seguridad de la Información El Artículo 2.2.22.3.8 Comités institucionales de gestión y desempeño del Decreto 1499 de 2017 establece “En cada una de las Empresas se integrará un Comité Institucional de Gestión y Desempeño encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG. Los Comités Institucionales de Gestión y Desempeño cumplirán las siguientes funciones: ... 6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.”, por lo tanto, el Comité Institucional de Gestión y Desempeño de la EIS CÚCUTA SA E.S.P. o a quien este delegue tiene bajo su responsabilidad asegurar la implementación y desarrollo de la política de seguridad digital y de la información. El subproceso de Gestión de Soporte y apoyo Informático, implementa y mantiene con el apoyo de las partes interesadas.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 11 de 35

POLÍTICA DE ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO

La Jefatura Administrativa, Financiera y Comercial, es la responsable de la adquisición, implementación y mantenimiento de todos los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), requeridas para los procesos de la Empresa, buscando, dentro del marco legal que rija, asegurar la calidad de los servicios entregados y de acuerdo con criterios de innovación, confiabilidad, disponibilidad, seguridad, economía e interoperabilidad, que den soporte a la productividad de los colaboradores, consultores, contratistas, terceras partes en los procesos.

Estándares de la Política de adquisición, implementación y mantenimiento de las TIC

Requerimientos tecnológicos: Cuando un área requiera implementar un software, plataforma tecnológica o sistemas de información, debe realizar la solicitud necesidad.

Desarrollo de aplicaciones: Las aplicaciones que desarrollen los colaboradores, consultores, contratistas, terceras partes, deben cumplir con los requerimientos de seguridad establecidos por la Empresa conforme con la Política de Seguridad de la Información, que se desarrolla más adelante en este documento.

La propiedad intelectual de los desarrollos contratados o realizados por los colaboradores, consultores, contratistas, terceras partes, dentro de su trabajo será propiedad de la Empresa, salvo acuerdo escrito expreso que diga lo contrario.

Los colaboradores, consultores, contratistas, terceras partes, que tengan acceso a los sistemas TIC de la Empresa, no podrán copiar ni ceder sin autorización las aplicaciones que son propiedad de la compañía ni las aplicaciones o programas de los que esta tenga licencia de uso.

Procesos de desarrollo y soporte: El proceso de adquisición y desarrollo de las aplicaciones debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones.

La documentación de cada uno de los sistemas implantados en la Empresa debe contener la guía para brindar soporte, la cual incluya copia del contrato con el proveedor que lo brinda, en caso de que aplique esta modalidad, especificando los Acuerdos de Nivel de Servicio (ANS) establecidos, los interlocutores y los procedimientos para obtener el servicio.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 12 de 35

Seguridad en los archivos del sistema: El acceso a los archivos del sistema y al código fuente debe ser restringido. La actualización del software aplicativo y las librerías solo pueden ser llevadas a cabo por los administradores, considerando que para software de proveedores las actualizaciones y migración a nuevas versiones se deben realizar antes de que termine la vigencia del soporte.

Los procedimientos de control de cambios deben estar documentados y ser ejecutados bajo los controles adecuados para no comprometer la seguridad de los sistemas.

Controles criptográficos: La implementación de controles criptográficos se realiza con base en una evaluación de riesgos que identifique el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido.

POLÍTICAS DE SEGURIDAD

La EIS CÚCUTA SA E.S.P. concede a los funcionarios diferentes recursos o servicios, para facilitarle la realización de las labores, siendo estos recursos o servicios propiedad de la empresa por tanto, los funcionarios tienen obligaciones y responsabilidades por el trato adecuado, siempre resguardando que no se haga mal uso o abuso de los mismos, razón por la cual las siguientes Políticas se refieren al uso adecuado que deben recibir dichos recursos o servicios que la institución presta a los funcionarios evitando las vulnerabilidades que afecta la disponibilidad, confidencialidad e integridad. Igualmente, la oficina de Sistemas de Información, deberá velar por el cumplimiento de éstas.

Teniendo en cuenta lo anteriormente expuesto, se hace necesaria la realización de unas políticas de seguridad, que serán de gran ayuda para el correcto funcionamiento de los equipos de cómputo.

POLÍTICA PARA EL USO ADECUADO DE ESTACIONES DE TRABAJO

La EIS CÚCUTA SA E.S.P. asigna a los funcionarios que por medio del área de Gestión Tecnológica entrega para el cumplimiento de sus labores, cuando se requiere una estación de trabajo. Estos equipos son parte del patrimonio

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 13 de 35

institucional y por lo tanto debemos buscar la mejor forma de utilizarlos, tomando en cuenta aspectos de seguridad físicos y lógicos para su protección. Las normas asociadas a esta política incluyen entre otras, las mejores prácticas de uso de las estaciones para proteger el equipo y la información contenida en él.

Instalación de Equipos

- Los equipos de cómputo (computadores, sitios de trabajo, servidores y demás equipos) deben tener una instalación adecuada acorde con cada una de las diferentes partes así como las partes eléctricas, por ejemplo, los dispositivos de cómputo siempre deben estar sobre las superficies de trabajo, para que el manejo y control del equipo sea el mejor.
- Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.
- No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia del subproceso de gestión de soporte y apoyo informático el retiro o cambio de partes y/o componentes.
- Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, en el caso de ser necesario, debe ser notificado tanto a Almacén como a la oficina de gestión de soporte y apoyo informático para su respectivo control.
- Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente, regulada, fase neutro y polo a tierra.
- La oficina de Gestión de Soporte y Apoyo informático, debe realizar la hoja de vida de los equipos de cómputo para llevar un control de los equipos propiedad de la empresa, en donde se manifieste el usuario que tenga asignado el equipo bajo su responsabilidad.
- La oficina de gestión de soporte y apoyo informático deberá especificar las características necesarias para la adquisición de equipos de acuerdo a su operación y funcionamiento.
- Al responsable del equipo se le asigna un usuario con la respectiva contraseña, independiente del usuario administrador que ejerce control sobre las configuraciones específicas del equipo.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 14 de 35

Manipulación de Equipos

- La infraestructura tecnológica (servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general) no puede ser utilizada en funciones diferentes a las empresariales.
- Ningún funcionario a excepción de la oficina gestión de aporte y apoyo informático se encuentra autorizado para manipular los componentes de los equipos de cómputo.
- La manipulación, daños y partes faltantes son de responsabilidad del usuario a quien se le asignó el equipo, quien deberá controlar el acceso a las demás personas no autorizadas debido a que el equipo está a su cargo.
- Los equipos deben ser manipulados de tal manera que cumplan y satisfagan las tareas a las cuales fueron designados, debido a cada una de las funciones y programas instalados, con el fin de realizar el cumplimiento de las actividades designadas.
- Los equipos deben ser manipulados de la forma en la que se encuentra situadas sus partes con el fin de que no existan fallas tanto eléctricas como funcionales debido a los movimientos bruscos o por la ubicación incorrecta de sus partes.
- La manipulación de los equipos también incluye la revisión de los equipos con fallas causadas por la mala conexión o falta de conexión eléctrica que puede ser realizadas por los mismos usuarios sin hacer solicitud a la oficina de Gestión de Soporte y Apoyo informático.
- La utilización de los equipos es con fin de trabajo; no se pueden realizar descargas de otra serie de software ajeno a las actividades informáticas de la oficina.
- No es permitido destapar o retirar la tapa de los equipos, ni podrá retirar o instalar partes sin la autorización de la oficina de Gestión de soporte y apoyo informático.
- Ningún funcionario podrá formatear los discos duros de los computadores, sin previa autorización de la oficina de Gestión de Soporte y Apoyo informático.
- Antes de desconectar cualquier dispositivo del computador, se debe desconectar previamente del equipo, en caso contrario, se puede perder datos, o incluso dañar el dispositivo, haciendo inaccesible todo el contenido.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 15 de 35

- No es recomendable guardar ningún dispositivo de almacenamiento magnético de información cerca de ninguna fuente electromagnética, como altavoces, transformadores, etc.

Buenas prácticas frente a un computador

- Mantener limpio de polvo el computador y libre de otros objetos, de modo que no se obstruya ningún punto de ventilación, pues a través de las ranuras de la CPU capta el aire del exterior para la refrigeración de los distintos componentes. Igualmente, se debe tener la prevención con los periféricos.
- Por seguridad en el lugar de trabajo, la espalda debe estar recta y los pies apoyados en el suelo, con el fin de prevenir problemas en la columna.
- Mantener los codos con un ángulo de 90 grados del teclado y mouse para que las muñecas no estén flexionadas y apoyadas para evitar dolores en las articulaciones de la mano y futuras complicaciones.
- No comer, fumar ni ingerir líquidos frente el computador para evitar incidentes y accidentes, además, por su salud se evita adquirir bacterias y en algunos casos prevenir la obesidad.
- Mantener una distancia mínima de 55 cm de la pantalla y los ojos deben estar a la misma altura que el borde superior de la pantalla con el fin de prevenir cansancio en los ojos, posible problemas con la visión, dolores de cabeza, espalda o cuello.
- No golpear ni mover bruscamente los equipos ni sus periféricos.
- Se aconseja utilizar colores claros y mate en la pantalla para evitar cansancio en la vista.
- La posición del monitor debe evitar que la luz incida directamente sobre la pantalla para prevenir daños a causa del reflejo de la misma y, al mismo tiempo, evitar una visualización incómoda.
- Evitar limpiar la pantalla con productos que puedan dañarla como alcohol o jabones, se aconseja usar un trapo de tela suave ligeramente humedecido y no hacer fuerza excesiva durante la limpieza.
- En el caso de personas zurdas han de cambiar la posición del ratón al lado izquierdo del teclado y configurarlo así en las propiedades del ratón desde el Panel de Control.
- Mantener los equipos apagados mientras no se estén utilizando.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 16 de 35

Mantenimiento de Equipos

- La conservación de los equipos, su funcionamiento, la seguridad física de cada equipo hacen parte de las responsabilidades de los usuarios.
- La instalación de cada uno de los equipos conforme al sitio y espacio de trabajo, el mantenimiento preventivo y correctivo es responsabilidad de la Oficina de Gestión de Soporte y Apoyo informático.
- Está prohibido que los equipos informáticos sean atendidos por personal ajeno a la Oficina de Gestión de Soporte y Apoyo informático para el mantenimiento preventivo y correctivo. El funcionario responsable del equipo responderá por daños adversos a estos mantenimientos o arreglos realizados por terceros.
- Los usuarios también hacen parte del mantenimiento de los equipos de cómputo haciendo un buen uso y utilidad de los equipos para que su funcionamiento sea el mejor y los mantenimientos preventivos y correctivos se prolonguen con la ayuda de la buena manipulación.
- Las solicitud se debe buscar por medio del sitio web a la oficina de gestión de soporte y apoyo informático en el formato respectivo de mantenimiento correctivo, desde el momento que el equipo este fallando y las precauciones realizadas por el usuario no hayan sido satisfactorias para que el equipo funcionara.
- Es estrictamente obligatorio, informar oportunamente a la oficina de gestión de soporte y apoyo informático, la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, o cualquiera otra, que altere la correcta funcionalidad.
- Queda rotundamente prohibido realizar mantenimiento preventivo y correctivo a equipos ajenos a la empresa.

Actualización de Equipos

- Los equipos de cómputo (computadores, sitios de trabajo, servidores y demás equipos), y equipos de red que sean propiedad de la EIS CÚCUTA SA E.S.P. se debe actualizar de manera periódica manteniendo las funcionalidades necesarias por el usuario, con el fin de aumentar la calidad de servicio, actividades y atención por cada uno de los usuarios y responsables de los equipos, aumentando su desempeño.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 17 de 35

POLÍTICA PARA EL USO DE EQUIPOS DISPOSITIVOS MÓVILES

La EIS CÚCUTA SA E.S.P establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas), entre otros suministrados por la Empresa y personales que hagan uso de los servicios de información

Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes y tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones y las actividades de los colaboradores de la Empresa en el ejercicio de sus funciones o de sus obligaciones contractuales.

Se autoriza el uso de WhatsApp pero no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

POLÍTICA DE EQUIPOS TIPO PORTÁTIL

La EIS CÚCUTA SA E.S.P. asigna equipos tipo portátil a sus funcionarios, para facilitarles el cumplimiento de sus labores. Los funcionarios que tengan asignado cualquier equipo tipo portátil, deben hacer correcto uso de los mismos y de la información que contienen, porque dadas las características de ese tipo de tecnología, se presentan más vulnerabilidades de seguridad, por las facilidades de conectarse diferentes ambientes informáticos, y adicionalmente son más susceptibles a robo o pérdida, Los colaboradores, consultores, contratistas y terceras partes, podrán hacer uso de los dispositivos móviles, siempre y cuando cumplan con los criterios técnicos, funcionales, de seguridad, regulatorios, establecidos por la Empresa.

- Asegurar el equipo portátil cada vez que deje de utilizarlo, en lo posible guárdelo en un lugar que cuente con unas medidas mínimas de seguridad.
- Cada vez que descargue algún archivo a su equipo portátil, utilice siempre la aplicación de antivirus para revisar su contenido. Normalmente el antivirus automáticamente revisa cualquier tipo de archivo. Si desea realizar un escaneo de archivos manual, podrá contactarse con la oficina de soporte y apoyo informático.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 18 de 35

- Para reportar cualquier incidente de seguridad (ya sea virus, SPAM, otros) deberá comunicarse con Gestión de Soporte y Apoyo informático para minimizar los daños. No reenvíe archivos desde su computador si sospecha que este pueda estar infectado, en estos casos desconecte el equipo de la red de datos hasta que se le indique lo contrario.
- Los equipos portátiles asignados a las oficinas son de uso exclusivo para los funcionarios que laboran en la EIS CÚCUTA SA E.S.P. ya sea de planta o contratista, no es aceptable el uso de los mismos por familiares y/o amigos.
- Evite dejar el equipo portátil con la sesión abierta. Siempre apague, bloquee (teclas Windows + L) o active el protector de pantalla con contraseña después de utilizar activamente el equipo.
- Únicamente el personal de la oficina de gestión de soporte y apoyo informático está autorizado para instalar algún tipo de software en el equipo portátil.
- El usuario se hará responsable directo de cualquier mal uso, mientras tenga a su cargo el computador portátil y sus accesorios.
- Todo dispositivo electrónico de almacenamiento que se conecte al equipo debe ser analizado con el antivirus inmediatamente se conecte, no es recomendable acceder al contenido sin ser previamente analizado.
- Cuando sea necesario el traslado de los equipos portátiles ya sea en las instalaciones de la EIS CÚCUTA SA E.S.P. o fuera de ellas debe estar debidamente apagado, y en el bolso asignado. Recuerde asegurar el equipo portátil cada vez que deje de utilizarlo, en lo posible guárdelo en un lugar seguro.
- Cuando sea necesario el traslado de los equipos portátiles fuera de las instalaciones de la Empresa debe ser registrada tanto la salida como la entrada en la portería de la empresa.
- Es responsabilidad de los colaboradores, consultores, contratistas, terceras partes, hacer un uso adecuado de éste servicio. Asimismo, deben acogerse las disposiciones de navegación definidas por la compañía que prohíben la consulta de páginas violentas, pornográficas o que atenten contra los principios, ética y moral de los colaboradores, consultores, contratistas, terceras parte. El incumplimiento por parte de los colaboradores, consultores, contratistas, terceras partes, de lo dispuesto en esta Política, dará lugar a las sanciones previstas en el Código Sustantivo del Trabajo, el Reglamento Interno de Trabajo, el Contrato de Trabajo Individual y en otras leyes y normas que resulten aplicables.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 19 de 35

POLÍTICA PARA LA SEGURIDAD DE EQUIPOS DE PROPIEDAD DE CONTRATISTAS

Por medio de esta política se dictan los lineamientos para el uso de equipos de propiedad de contratistas que hacen uso de los recursos y servicios tecnológicos de la EIS CÚCUTA SA E.S.P.

- Antes de conectar por primera vez equipos o dispositivos a la red LAN corporativa se debe solicitar su autorización de conexión al subproceso de gestión de soporte y apoyo Informático para el debido análisis, aprobación o no y registro en la base de datos de control de equipos de terceros que usan la infraestructura tecnológica de la Empresa.

Para los equipos que no son propiedad de la EIS CÚCUTA SA E.S.P., y es requerida su conexión a la red corporativa se debe informar al propietario los requisitos requeridos en el equipo para su incorporación a la red corporativa y el acceso a sus recursos.

- Todo equipo o dispositivo conectado a la red corporativa debe tener actualizado y con licencia legal: o Antivirus o Sistema operativo y mecanismo de actualizaciones automáticas de seguridad o Suite ofimática.

POLÍTICAS PARA EL USO DE PROYECTORES

La EIS CÚCUTA SA E.S.P. cuenta con proyectores para mostrar las presentaciones, conferencias y/o videoconferencias propias de las actividades realizadas por los diferentes Procesos y subprocesos.

Se debe tener en cuenta que la lámpara de un proyector es muy delicada y de alto costo. Además de seguir las siguientes sugerencias, se recomienda leer el manual de usuario del equipo para evitar una mala manipulación.

- a) Cuidar el lente de los proyectores, para evitar que el lente se ralle o quede con marcas de grasa, no tocar el lente del proyector con los dedos, ni con otros objetos, ni limpiar el lente con papel (sólo utilizar paños secos y suaves, que no dejen pelusas).

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 20 de 35

b) Cuidar la lámpara de proyectores. Para evitar que la lámpara de un proyector se queme, siga los siguientes consejos:

- Nunca desconecte el proyector de la energía eléctrica cuando esté encendido o esté en proceso de apagado para evitar que se queme la lámpara.
- Al momento de desconectar el Proyector, independiente de la marca y modelo, es preciso esperar hasta que el ventilador termine de enfriar la lámpara antes de ser desconectado de la energía eléctrica. En algunos modelos, que cuentan con la característica de “Apagado Instantáneo”, “Apagado Rápido” o “Instant off”, esto tarda sólo unos segundos, y generalmente es avisado por una alarma sonora.
- Evitar dejar cables sueltos en el área de circulación de la sala o mal conectados al enchufe o al proyector.
- Cuidar la ventilación de los proyectores. No obstruir las ranuras de ventilación del equipo con ropa, papeles, u otros objetos. Esto puede causar el recalentamiento del proyector, e incluso quemaduras o un incendio.

POLÍTICAS PARA EL USO DE RECURSOS DE RED

El uso de Internet, impresoras y documentación se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, por lo tanto cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la Empresa, cualquier uso para otros propósitos no es aceptable. El usuario deberá considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

Internet

- La utilización del internet se debe hacer de forma segura contando con una disponibilidad de internet compartido el cual se utiliza con fines de trabajo y no sociales.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 21 de 35

- El acceso a internet es de manera laboral, por lo tanto queda prohibido el uso de internet para navegar en zonas restringidas y no permitidas como también queda prohibido el uso del internet para el acceso a redes sociales ya que el rendimiento del internet se puede ver afectado por estas conductas.
- El internet se utiliza con fines de trabajo por lo tanto no se pueden hacer descargas de archivos y software, ya que esto puede afectar el rendimiento de las conexiones a internet, no se debe acceder a la visualización de páginas en línea con contenido inadecuado esto afectara el rendimiento de la computadora y la rapidez de la red.
- Se encuentra prohibido el acceso a sitios pornográficos, sitios religiosos dedicados a difundir las creencias de alguna religión o secta en particular, acceso a sitios web de alzados en armas o de grupos terroristas a nivel nacional o internacional dedicados a difundir temas relacionados con violencia.
- El internet inalámbrico se utiliza con el fin de dar soporte únicamente a las computadoras que no pueden tener acceso directo debido a los lugares donde se encuentran o porque los dispositivos no cuente con periféricos de red, por lo tanto, queda prohibido el compartimiento de las claves de acceso a las redes inalámbricas.
- Los usuarios de la institución deben tener precauciones a la hora de navegar en internet debido a la existencia de software malicioso y virus que se propagan por el internet, los cuales puede ser causante de fallas en los equipos de cómputo y perdida de información.
- Nunca hacer clic en enlaces que vengan de un remitente desconocido, aunque resulten atractivos, pues lo más seguro es que no se obtenga lo deseado y además infecte con un virus el computador.
- Al entrar en páginas donde se deba facilitar datos confidenciales, se deben asegurar de acceder con protocolo https, las del final significa Secure (segura) y la transmisión de la información irá cifrada.
- Comprobar que en el navegador aparece un candado que nos asegure la validez del certificado y que este no ha caducado.
- Verificar los dominios o links de las páginas web en caso de recibir mensajes de Empresas bancarias o ente gubernamental
- No abrir banners publicitarios

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 22 de 35

Impresoras

- Evitar dejar documentos en cola, al haber varios imprimiéndose pueden causar una saturación de las tareas de la impresora.
- Con las impresoras multifuncionales se debe tener precaución a la hora de enviar documentos a ser escaneados debido a que se debe escoger el equipo en el cual debe quedar el documento escaneado.
- Verificar que tanto la impresora como el equipo a la cual se encuentre conectada esté encendido o tenga el cable de red conectado de manera correcta para que su funcionamiento sea el más óptimo.

Documentación

- Precaución de hacer buena utilización de la documentación, debido a que esa documentación es de apoyo y de trabajo de varias personas.
- Precaución al guardado de una copia de la documentación de forma local, la cual nos ayudara y será de fortaleza si pasa algo o la red no funciona de manera adecuada.
- Precaución a la hora de compartir documentación en la red en la cual se debe seleccionar los beneficiados para que no sea compartida con todos los usuarios ya que para todos no son de utilidad y pueden generar pérdidas o suministrar documentación a terceros.
- Precaución a la hora de hacer el guardado de la documentación si está siendo utilizada de forma remota por varias personas las cuales pueden hacer modificación y las cuales no pueden ser guardadas por acciones de otro usuario que la esté trabajando y niegue su guardado.

POLÍTICA LINEAMIENTO DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL LAN)

El objetivo de esta política es asegurar la correcta y segura operación de los puntos de red.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 23 de 35

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales o equipos de contratistas debidamente autorizados.
- Los equipos de visitantes, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y redes WIFI definidos por el Líder de Gestión de Soporte y Apoyo Informático de la Empresa.

POLÍTICA DE CONTROL DE ACCESO

La EIS CÚCUTA SA E.S.P. asigna a cada funcionario en apoyo al cumplimiento de sus labores dando acceso a equipos informáticos, a la red de datos institucional y a documentación, con la cual el empleado puede acceder diferentes elementos que la componen como: servidores de archivos, servidores de bases de datos, impresoras, archivos compartidos en otras estaciones de trabajo, sistemas y aplicaciones Institucionales, entre otros. Por lo anterior, los empleados deben hacer uso de la red y de los servicios relacionados con esta, estrictamente en cumplimiento de las labores de la Empresa, tomando en consideración la privacidad de otros usuarios y la no saturación de la red por uso indebido del ancho de banda, ningún empleado está autorizado para crear claves, cuentas de usuario, instalar programas y realizar modificaciones a los equipos sin autorización de la persona encargada de la oficina de gestión de soporte y apoyo informático.

Control de acceso a equipos informáticos

- Todos los equipos de cómputo tienen asignado un responsable y un usuario, debe cumplir con la responsabilidad de darle buen uso y funcionamiento a los equipos.
- Los equipos de cómputo que se encuentren en áreas críticas donde sea de fácil acceso deben tener un seguimiento y deben poseer su respectiva seguridad.
- Los cuartos de Rack son áreas donde se encuentren los equipos imprescindibles para el funcionamiento y trabajo en los departamentos de la Empresa, el cual, se encuentra restringido el acceso a los funcionarios ajenos a la oficina de gestión de soporte y apoyo informático.

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 24 de 35

- El servidor de datos, es para almacenamiento de base de datos de sistemas de información estos archivos permitirán la continuidad del servicio.
- Las impresoras no son para uso personal, se prohíbe la impresión total o parcial de información ajena a la EIS CÚCUTA SA E.S.P.
- Los equipos con acceso a la red institucional, el internet no podrán usar el ancho de banda para ver videos, escuchar música o acceder a redes sociales, ya que el uso del internet es estrictamente necesario para cumplir las labores del cargo.
- Está restringido el uso de programas de descarga de contenido audiovisual (música, videos, fotos) y software, que no apoye el desarrollo de las funciones laborales para cumplir la misión de la institución.

Control de acceso a la red local.

- Gestión de Soporte y Apoyo informático es responsable de dar acceso a un punto remoto, en el cual es asignada una dirección IP dentro del rango de direcciones que la Empresa tiene para ofrecer conectividad a internet y recursos compartidos.
- Los usuarios deben hacer utilización de la red local de manera adecuada (no acceder a información ajena y no utilizar recursos de red que no estén permitidos) para que el funcionamiento y la realización de las tareas sean las mejores.
- Gestión de soporte y apoyo informático es el encargado de visualizar y realizar prevención del buen uso de la red.
- El acceso a los equipos de cómputo especializados como servidores y equipos de red se deben hacer por medio del personal autorizado por gestión de soporte y apoyo informático.
- Los equipos que son de la Empresa y sean conectados a la red local, o aquellos que sean conectados a la red inalámbrica debe hacer uso de la misma de manera responsable y con la mejor de las disposiciones para el buen funcionamiento de las redes.

Control de acceso a la documentación

- El control de acceso a la documentación que es compartida en red se debe hacer de manera segura y con precauciones de guardar una copia en el equipo del usuario.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 25 de 35

- La información que se encuentre en la red se debe proteger y utilizar solo con fines laborales, no con fines personales ni de lucro, ni transferir a terceros, los cuales podrían utilizar la información con otros fines como dañar la Empresa.
- Se considera falta gravísima al detectar los usuarios que vulnere la información contenida en los equipos de cómputo o en la red institucional como borrar carpetas compartidas o no autorizadas.

POLÍTICA PARA USO DE SOFTWARE

Instalación del Software

- Los usuarios no pueden instalar, suprimir o modificar el software originalmente entregado en su computador. Es competencia de gestión de soporte y apoyo informático.
- Es responsabilidad de gestión de soporte y apoyo informático dar a conocer las bases y los tipos de software que se deben instalar.
- Las cualidades y características del software que se debe instalar en los equipos de cómputo de la EIS deben cumplir con características de soporte para las actividades de desempeño laboral y contar con un licenciamiento.
- En la instalación de software nuevo en los equipos de cómputo Gestión de Soporte y Apoyo informático deben tener estudio pleno y responsabilidad en la instalación ya que puede estar en riesgo tanto la información de trabajo del usuario, también es responsabilidad del usuario realizar las respectivas copias de seguridad de la información.
- Gestión de y apoyo informático es el responsable de la instalación de software de seguridad de los equipos de cómputo como los son antivirus, vacunas, privilegios de acceso y otros software que ayuden con la protección del equipo información del usuario.
- La seguridad lógica y física de los equipos compete al funcionario a quien es asignado el equipo.
- Compete al usuario hacer uso propio del software instalado solo con fines laborales, no con fines de lucro personal como también es de responsabilidad dar a conocer novedades que se presenten con el software instalado a gestión de soporte y apoyo informático.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 26 de 35

Actualización del Software

- La actualización y adquisición de nuevos software para los equipos de cómputo es de responsabilidad de Gestión de Soporte y Apoyo informático por lo tanto queda prohibido la actualización de software sin previo aviso.
- Está prohibido la intervención de personal ajeno a gestión de soporte y apoyo informático para realizar instalación o actualizaciones de software.
- Si se presenta una actualización o una notificación del equipo de cómputo al usuario para hacer actualización es de suma responsabilidad del usuario comunicarse con gestión de soporte y apoyo informático para que sea guiado y apoyado para la respectiva actualización.

Software Legal

- Los computadores se deben adquirir con la respectiva licencia del Sistema Operativo.
- Es responsabilidad del usuario hacer uso de software legal y con su respectiva licencia.
- Le corresponde al usuario informar y dar a conocer sobre el vencimiento de las licencias del software que posee el equipo de cómputo.
- El usuario es responsable de todo software instalado sin autorización de gestión de soporte y apoyo informático, como también de las consecuencias que cause la instalación de software ilegal y con virus.
- Se debe informar al Almacén cuando se ha terminado la vida útil del software o la licencia haya caducado y no se actualiza para que sea tenido en cuenta en el Comité para dar de baja al bien intangible.

Uso de plataformas de Software

- Cualquier software que sea de uso institucional debe ser instalado por gestión de soporte y apoyo informático.
- El software que se usa institucionalmente y que es manipulado por los usuarios, deben hacer utilización del software de manera exclusiva para las labores y actividades trabajo de la EIS.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 27 de 35

- El software que requieran ser instalados para el trabajo en red de la institución debe ser evaluado con anticipación como también la capacitación en la utilización a los usuarios.
- Es responsabilidad del usuario realizar buenas practicas con el software que posee la Empresa con el fin de aprovechar los beneficios y riquezas que ofrecen el software.(Consultar los manuales de usuario)
- Se debe dar a conocer por parte de los usuarios a gestión de soporte y apoyo informático las fallas y no funcionamiento correcto de software.

Mecanismo de control de Software

- Perfiles de usuarios con acceso restringido para la instalación y desinstalación de software.
- Verificación aleatoria de software instalado en los equipos de las diferentes dependencias u oficinas, en caso de existir software no licenciado se procede a la desinstalación del mismo.
- Se da instrucciones a los funcionarios sobre el uso del hardware y software, enfatizando en la responsabilidad y consecuencias que conlleva la instalación de software no licenciado.

POLÍTICA PARA EL USO DE UNIDADES DE ALMACENAMIENTO DE INFORMACIÓN

La información constituye uno de los principales activos de la EIS, por tanto el manejo adecuado de la misma es responsabilidad de todos los funcionarios así como la correcta utilización de los dispositivos que el mercado ofrece para la administración y respaldo información. Por lo tanto, todos los usuarios de tecnologías de información que manipulen dispositivos de almacenamiento deben utilizarlos considerando la importancia de la información que contienen, buscando mecanismos seguros para su almacenamiento o distribución

Teniendo en cuenta la importancia de la información que maneja la EIS y la necesidad de resguardar los datos, así como emitir información a otras Empresas, surge la necesidad de establecer la normativa para regular el uso de cualquier tipo de unidades de respaldo sean internas o externas, entre las que podemos

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 28 de 35

mencionar los quemadores de discos compactos, DVD, memorias USB, Disco Duros interno y externos entre otros; con el objeto de que su uso sea para labores propias de la empresa.

Por lo anterior, toda unidad que cuente con dispositivos para la realización de respaldos (computadoras de escritorio, portátiles y servidores) debe velar porque se haga un uso adecuado de esos recursos, utilizándolos únicamente para cumplir con los intereses de la EIS, y tomando en cuenta las funcionalidades operativas del equipo.

- No se permite realizar copia no autorizada de material protegido por derecho de autor.
- No se permite almacenar información de índole personal como videos, fotos, música entre otros, en los equipos institucionales.
- No se permite modificar, eliminar o copiar un archivo perteneciente a otro Usuario sin el previo consentimiento del dueño del archivo.

Organización de la información en un equipo de cómputo

- El usuario deberá crear una carpeta con el nombre del equipo, en el disco local C y guardar toda la información en dicha carpeta.

Nombre de los archivos

- Se recomienda no guardar archivos con nombres muy largos. Es de vital importancia a la hora de realizar una copia de seguridad, pues en ocasiones, los archivos que tienen nombres muy largos ocasionan problemas y no permiten su manipulación.
- Es importante nombrar los archivos con nombres que permitan reconocer el contenido. Con el fin de evitar la revisión de todos los archivos que están en el computador abriéndolos, sino que simplemente se pueda limitar a leer el nombre del archivo, y con esto tomar la decisión si se guarda o se elimina.
- Tener en cuenta que algunos Sistemas Operativos no permiten ingresar unos caracteres especiales al nombre del archivo, por tanto, se sugiere **NO** nombrar archivos o carpetas utilizando caracteres especiales como (#\$%&?'|¿).

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 29 de 35

Organización de los Archivos

- Se recomienda llevar control y orden de los archivos, con el fin de aprovechar el espacio del equipo de cómputo y facilitar la búsqueda de información.
- No se recomienda crear demasiadas subcarpetas, ya que al momento de realizar copias de seguridad el sistema operativo incluye la ruta del archivo como si formara parte del nombre del archivo.
- Grabar cambios de archivos frecuentemente. Al trabajar con documentos de texto, planillas de cálculo u otro archivo, se recomienda guardar los cambios frecuentemente para evitar pérdida de los avances frente a un apagado inesperado del equipo. En lo posible, utilizar versiones de los archivos en la medida que se generan modificaciones en ellos.

POLÍTICA DE COPIAS DE SEGURIDAD

La realización periódica de respaldos de la información generada en los sistemas, bases de datos, así como la información residente en los equipos de los funcionarios de la EIS CÚCUTA SA E.S.P. es de gran importancia para brindar continuidad de los servicios. Por lo tanto, todos somos responsables de su preservación.

- a) Las copias de seguridad Backup and **Sync** está destinada principalmente a usuarios finales de PC's. Es un sistema de sincronización que nos permite subir a la nube todo nuestro ordenador o sólo sincronizar carpetas específicas, en el caso para la Empresa de Acueducto y Alcantarillado SA E.S.P, se cuenta definida según programación cada tres días(Lunes, Miércoles y viernes), la información es encriptada y se sube al almacenamiento de la nube en diferentes versiones, cada vez que se realice se crea una versión de la misma eso dependiendo de los cambios que hayan entre copias, cuando se realice el proceso de restauración se tiene que desencriptar a través de una clave para desencriptar.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 30 de 35

- b) Las copias realizadas al servidor se hacen a través de un dispositivo NAS QNAP NAVIO, estas se realizan diariamente, y se reemplaza el día anterior
- c) Cada funcionario debe salvaguardar la información que se encuentra bajo su responsabilidad, y es su deber informar en dado caso de alguna alerta presentada en su equipo.

POLÍTICA DE USO DE TELEFONÍA IP

Telefonía Fija

La asignación de extensiones telefónicas y modificación de categorías de acceso telefónico se hará de acuerdo con el perfil configurado en la matriz de atributos.

El uso de los teléfonos fijos asignados a los colaboradores debe ceñirse al desarrollo de actividades relacionadas con el cargo.

- Todos los servicios, requerimientos o incidentes, después de pasar por los niveles de autorización establecidos, serán canalizados por medio de la Mesa de Ayuda, hacia el proveedor de Outsourcing de telecomunicaciones.

Tele presencia

La Empresa dispone de licencias para videoconferencia en Meet para establecer contacto virtual entre los colaboradores, consultores, contratistas, terceras partes, de la Empresa, permitiendo acortar distancias y hacer más eficientes los procesos.

POLÍTICA DE USO DE CORREOS ELECTRÓNICOS

Se debe tener en cuenta los siguientes lineamientos para el uso del correo electrónico institucional de la EIS CÚCUTA SA E.S.P.:

- a) Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 31 de 35

forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

- b) El sistema de correo electrónico institucional debe ser usado únicamente para propósitos laborales.
- c) El servicio de correo electrónico de la Institución no debe ser utilizado para enviar correo basura (Spam).
- d) Es necesario crear una rutina diaria de limpieza de correos leídos, los cuales, deben ser archivados de acuerdo a la TRD institucional.
- e) Si desea almacenar los correos o contar con un Backup (copia) de los mismo, es necesario hacer el re direccionamiento de la cuenta a una cuenta externa, ya sea (Gmail, Hotmail, Yahoo u otra), la solicitud la puede realizar a gestión de soporte y apoyo informático.
- f) Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar los lineamientos y recomendaciones para dicho tipo de documentos, tales como:
 - Iniciar su correo con un saludo formal.
Ejemplo: Buenos días o Doctor.... Cordial saludo.
 - Nombrar al destinatario de correo por su nombre o profesión.
 - Evitar el uso de palabras que puedan resultar ofensivas.
 - Escribir puntualmente.
 - No extenderse demasiado.
 - Al final del correo agradecer por la atención prestada y firmar. La firma debe contener nombre y apellidos completos, cargo dependencia, nombre completo de la Empresa, dirección de la oficina, teléfono de contacto, correo electrónico.
- g) Los usuarios del correo electrónico institucional no deben enviar mensajes personales u ofensivos; mensajes cadenas o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Institución.
- h) Los correos institucionales no deben ser inscritos en ninguna página para acceder a información en la web, ya que estas páginas usan los correos para enviar correos Spam o publicidad.
- i) Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra dependencia o línea. En caso de ausencias o vacaciones, se debe recurrir a Gestión de Soporte y Apoyo informático como mecanismo alterno para el envío de correos.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 32 de 35

- j) No abrir correos electrónicos de remitentes desconocidos, sin asunto, o cuyo asunto resulte sospechoso.
- k) Confirmar telefónicamente la procedencia de los correos nuevos y su contenido sin importar el origen, ya sea Empresa pública o privada.
- l) No abrir archivos adjuntos o links desconocidos que envíen a través de correo electrónico.
- m) No compartir información financiera ni personal a través de redes sociales, llamadas o mensajes.

POLÍTICAS INFRAESTRUCTURA INFORMÁTICA

Responsabilidades de la operación:

Los procedimientos de operación deben considerar la planeación de la operación, el tratamiento y manipulación de la información, las copias de respaldo, el manejo de errores o excepciones durante la ejecución de un trabajo, los contactos de apoyo para el caso de dificultades operacionales o técnicas inesperadas, reinicio de los sistemas y procedimientos de recuperación a utilizar en caso de falla del sistema, gestión de pistas de auditoría y sistemas de registro de información, y el aseguramiento de plataformas.

Separación de ambientes:

Para minimizar los riesgos en el proceso de puesta en producción de los cambios y nuevos desarrollos, así como el impacto por la no disponibilidad de los servicios, se debe establecer una segregación de ambientes, (Desarrollo, Pruebas y Producción), considerando:

- Definir y documentar las reglas para el paso de software entre ambientes.
- El uso de diferentes equipos, dominios y directorios.
- La restricción de uso de compiladores, editores y otras herramientas de desarrollo o recursos del sistema en ambientes de producción.
- Los sistemas de prueba deben emular al sistema productivo tan real como sea posible.
- El uso de perfiles de usuario diferentes para los diferentes ambientes.
- Los menús deben mostrar mensajes de identificación adecuados para reducir el riesgo de error.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 33 de 35

- La restricción de uso de datos de producción en ambientes de prueba. En caso de ser necesario se debe utilizar un mecanismo de enmascaramiento.

Almacenamiento en Nube–Cloud

El almacenamiento en la nube, debe garantizar que todos los datos de usuarios se almacenen de una manera central, y que la información no solo se almacene a nivel local, La Jefatura Administrativa, Financiera y Comercial, por medio del área de gestión soporte y apoyo informático.

Planificación y aceptación

Se deben establecer proyecciones de capacidad futura, para reducir el riesgo de sobrecarga del sistema, Se hará monitoreo al uso de los servicios de red y de los sistemas, con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con los Acuerdos de Niveles de Servicio y reducir el riesgo de posibles fallas.

Protección contra códigos maliciosos

Se deben implementar controles de detección, prevención, recuperación y concientización, con el fin de que los usuarios tengan protección frente a códigos maliciosos.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y acorde con la propiedad intelectual.

POLÍTICA DE SEGURIDAD DE LOS EQUIPOS

La política de Seguridad de los Equipos es asegurar la protección de la información en los equipos. Instalación de equipos de procesamiento y almacenamiento

- Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el líder de gestión de soporte y apoyo Informático.

 EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA S.A. E.S.P.	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 34 de 35

- Los equipos dispuestos a ser alojados en áreas seguras deben cumplir con los requisitos de alistamiento definidos por el líder de Gestión de Soporte y Apoyo Informático. , como lo es un sistema operativo con las actualizaciones de seguridad vigentes, el antivirus o mecanismo de protección contra virus, la instalación de software con licenciamiento legal.
- Protecciones en el suministro de energía a la red de energía regulada de los Cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- El cableado que transporta datos y de suministro de energía deberán estar protegidos contra la interceptación, interferencia o daños.
- El acceso a los centros de cableado (Racks), debe estar protegido.
- El líder de gestión de soporte y apoyo informático establecerá un plan de infraestructura de mantenimientos de equipos.
- La EIS CÚCUTA SA E.S.P, debe mantener contratos de soporte y mantenimiento de los equipos críticos y las garantías de los equipos de escritorio, portátiles y dispositivos móviles.
- Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas atendiendo la debida programación y autorización por parte del líder de gestión de soporte y apoyo Informático.

Gestión de seguridad en las redes

Las redes y la infraestructura de apoyo deben ser adecuadamente gestionadas y aseguradas para protegerlas de amenazas y para mantener la seguridad de los sistemas y aplicaciones.

Se deben implantar controles relacionados con la segmentación, gestión, monitoreo y detección de eventos, para asegurar la información que viaja por las redes.

CONTROL DE CAMBIOS					
VERSIÓN	FECHA	PÁGINA	APROBÓ		DESCRIPCIÓN DE CAMBIOS
			NOMBRE	CARGO	

	SISTEMA INTEGRADO DE GESTIÓN	Código: GSO-PO-01
	GESTIÓN ADMINISTRATIVA, FINANCIERA Y COMERCIAL.	Versión: 03
	Gestión de Soporte y Apoyo Informático	Fecha: 24/05/2023
	Políticas Seguridad de la información	Página 35 de 35

1	28/08/2021 1	34	VIANNY KARINA BUITRAGO S.	Apoyo de soporte y apoyo informático	Elaboración de la política
2	14/10/2022 2	34	VIANNY KARINA BUITRAGO S.	Apoyo de soporte y apoyo informático	Modificación de política de copias
3	24/05/2023 3	35	VIANNY KARINA BUITRAGO S.	Apoyo de soporte y apoyo informático	Modificación de la política general y estructuración del documento

Emitido por:	Revisado Por:	Aprobado Por:
VIANNY KARINA BUITRAGO S. Apoyo de gestión de soporte informático	RAFAEL TAMAYO VILLAMIZAR Líder SIG	CARLOS JOSÉ IBARRA RODRÍGUEZ Representante de la Dirección