HOSPITAL LOCAL DE AGUACHICA E.S.E.

NIT. 824.000.785-2

E.S.E. HOSPITAL LOCAL DE AGUACHICA

PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ENERO 2023

La información contenida en el presente documento debe ser socializada, conocida e implementada por todo el personal del servicio, con el fin de promover la actualización y estandarización de los procesos y procedimientos de la E.S.E HOSPITAL LOCAL DE AGUACHICA

CONTENIDO

OBJETIVOS

Definir las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio en el Hospital Local de Aguachica ESE.

ALCANCE

Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones.

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios de TIC, aplica a todos los niveles funcionales, organizacionales y a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a la entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, esta política aplica a toda la información creada, procesada o utilizada por el Hospital en la TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

RESPONSABLES

- **Alta Dirección**: Es el grupo de funcionarios de la entidad que aprueban las diferentes políticas y directrices con relación a las TIC. En este caso particular aprobarán o establecido para la administración del riesgo.
- **Responsables por procesos**: Son las personas encargadas de identificar, analizar y valorar los riesgos en la entidad por lo menos una vez al año.
- **Funcionarios**: Se encargan llevar a cabo los controles y ejecutar acciones para la administración de los riesgos identificados.
- **Control interno**: Realiza la evaluación y seguimiento a la política, procedimientos y controles.

MARCO LEGAL

- **Constitución Política de Colombia.** Artículos 15, 20, 23 y 74.

- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Ley 23 de 1982.** Sobre derechos de autor

- **Ley 44 de 2093.** Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).

- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos.

- **Ley 527 de 2099.** Por la cual se define y reglamenta el 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.

- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico

- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas

- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.

- **Ley 1450 de 2011.** Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

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

- **Ley 1753 de 2015.** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país".

- **Ley 1755 de 2015.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.

- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

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

- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- **CONPES 3854 de 2017.** Política Nacional de Seguridad digital.

- **CONPES 3995 de 2020**. Confianza y Seguridad Digital

- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- **Decreto 1287 de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.

- **Directiva 26 de 2020.** Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario.

- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

DEFINICIONES

A continuación, se presenta el glosario de los términos utilizados en el diseño de este documento:

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplica.

DESARROLLO DEL PLAN

DATOS DE LA INSTITUCION

Departamento	Cesar
Municipio	AGUACHICA
Código Habilitación	200110012601
Hospital	EMPRESA SOCIAL DEL ESTADO HOSPITAL LOCAL DE AGUACHICA
Nivel	1
Carácter	MUNICIPAL
ESE	SI
Habilitado	SI
Nit	824.000.785
DV	2
Red	Sur
Tipología	EMPRESA SOCIAL DEL ESTADO
Tipo Acto	ACUERDO
Número Acto	038
Fecha Acto	19/12/1996
Dirección	Carrera 7 # 2-160
Teléfono	095-5651854
Email Institución	gerencia@hospitallocalaguachica.gov.co
Email Adicional	sgerencia@hospitallocalaguachica.gov.co
Gerente	SAUL HERNANDEZ GUTIERREZ
Vinculación	PERIODO FIJO
Email: Gerente	sahergu70@hotmail.com

SEDES DE LA INSTITUCIÓN

Nombre de la institución	Código de Habilitación	Ubicación	
Hospital Local de Aguachica	200110012601	Carrera 7 N° 2-160	ZONA URBANA
Centro de Salud San Eduardo	200110012602	Carrera 32 # 10n-97	
Centro de Salud Idema	200110012610	Calle 15ª # 14-30	
Puesto de Salud Buturama	200110012603	Corregimiento Buturama	ZONA RURAL
Puesto de Salud Barranca Lebrija	200110012604	Corregimiento Barranca Lebrija	
Puesto de Salud Campo Amalia	200110012605	Corregimiento Campo Amalia	
Puesto de Salud Norean	200110012606	Corregimiento Norean	
Puesto de Salud Puerto Patiño	200110012607	Corregimiento Puerto Patiño	
Puesto de Salud Santa Lucia	200110012608	Vereda Santa Lucia	
Puesto de Salud Villa de San Andrés	200110012609	Corregimiento Villa de San Andrés	
Puesto de Salud Juncal	200110012611	Corregimiento Juncal	
Puesto de Salud Loma de Corredor	200110012612	Corregimiento Loma de Corredor	

RESEÑA HISTÓRICA

El Hospital Local de Aguachica, nace como un centro de salud ubicado en el Barrio San Eduardo Carrera 32 No 10N – 97, En ese entonces contaba con: Un médico (el S.S.O), Enfermera, Auxiliar de Enfermería, Odontóloga (S.S.O). Auxiliar de odontología, Bacterióloga, Auxiliar de Laboratorio, Un celador, y un auxiliar de servicios generales,

quienes brindaban la atención a los usuarios que allí asistían. Luego se da el proceso de descentralización de la salud en el Segundo Nivel de atención en el HOSPITAL JOSÉ DAVID PADILLA VILLAFAÑE, donde una parte del personal que laboraba en esta institución es trasladada para el primer nivel de atención.

El acuerdo No 038 del 19 de Diciembre de 1996 el concejo Municipal lo Convierte en HOSPITAL LOCAL DE AGUACHICA Empresa Social del Estado, de conformidad con el artículo 194 de la ley 100 de 1993, y el articulo 95 del decreto ley 1298 de 1994 y este personal es adoptado por dicha Institución.

Se convierte Empresa Social del Estado Hospital Local de Aguachica E.S.E Entidad pública, Descentralizada del orden Municipal de naturaleza especial con personería jurídica, patrimonio propio e independiente de la Administración Municipal y Autonomía Administrativa, adscrito al Departamento Administrativo de Salud de Aguachica.

HOSPITAL LOCAL DE AGUACHICA EMPRESA SOCIAL DEL ESTADO

¿QUIÉNES SOMOS?

El Hospital Local de Aguachica, E.S.E, es una organización social que contribuye con el mejoramiento del bienestar y calidad de vida de la población del Municipio de Aguachica

y del sur del Cesar, a través de la prestación de servicios de salud de primer nivel de complejidad, de manera diferenciada, con énfasis en la promoción y mantenimiento de la salud y la prevención de la enfermedad, consulta externa, urgencias, hospitalización, servicios diagnósticos y de apoyo complementario superando las expectativas de nuestros usuarios y su familia con calidad, accesibilidad, oportunidad, seguridad, eficiencia, satisfacción y humanización en los servicios de salud, mediante la excelencia humana profesional que facilita el crecimiento para el desarrollo empresarial y social.

El Hospital Local de Aguachica E.S.E, cuenta con doce sedes para la prestación de los servicios de salud de baja complejidad, tres centros adscritos en la zona urbana y nueve centros en la zona rural, con el fin de aumentar la cobertura en la atención primaria en salud a toda la comunidad del Municipio de Aguachica y sur del Cesar.

Los servicios ofrecidos en el Hospital Local de Aguachica E.S.E son realizados con los más altos estándares de calidad, con tecnología de punta, y con un Talento humano idóneo, garantizando a nuestros usuarios calidad, seguridad, oportunidad, accesibilidad, satisfacción y confiabilidad en cada uno de nuestros procesos; cuenta con los servicios habilitados en el REPS, con el cumplimiento de los requisitos mínimos para brindar seguridad a los usuarios y su familia según lo definido en la Resolución N° 3100 de 2019 y en el programa de auditoria para el mejoramiento de la calidad basado en estándares de acreditación.

DIRECCIONAMIENTO ESTRATEGICO

MISION

Prestamos servicios de atención primaria en salud con enfoque integral, orientado a la seguridad del paciente, la atención humanizada y la satisfacción de los usuarios y sus

familias. Contamos con tecnología avanzada en cada uno de nuestros procesos, con talento humano idóneo, altamente calificado, autónomo, responsable, estratégico, competitivo y motivado a brindar un servicio con calidad.

VISION

El Hospital Local de Aguachica E.S.E, será para el 2030, una empresa líder en la prestación Primaria en Salud con un modelo de atención integral en salud humanizada y de alta calidad, con acciones asociadas en la promoción y mantenimiento de la salud en cada curso de vida, en la atención integral materno perinatal, educación e investigación docencia servicio y la gestión de riesgo en salud de forma oportuna, accesible, garantizando la seguridad y satisfacción en los usuarios y sus familias.

PRINCIPIOS

Los principios adoptados por el Hospital Local de Aguachica, Empresa Social del Estado son:

- ✓ **Mejoramiento continuo:** La entidad aplicara todos los procedimientos técnicos e instrumentos gerenciales que le permitan responder oportunamente a los cambios del entorno, contando con un personal comprometido en la búsqueda de resultados excelentes en su gestión, mediante el cumplimiento de sus deberes con competencia diligencia y calidad.

- ✓ **Oportunidad:** Cumplir a tiempo y con calidad las funciones en la prestación del servicio a los usuarios.

- ✓ **Colaboración:** Los servidores públicos y/o contratista deben realizar aquellas tareas que por su naturaleza o modalidad sean las estrictamente inherentes a su cargo siempre que ellas resulten necesarias para mitigar, neutralizar o superar las dificultades que enfrente la empresa o nuestros clientes.

- ✓ **Eficacia:** Realización de actividades planificadas para alcanzar el logro de los resultados esperados.

- ✓ **Austeridad:** Los servidores públicos y/o contratistas del Hospital Local de Aguachica, Empresa Social del Estado, deben obrar con sobriedad y racionalización en el uso de los recursos, de tal manera que proyecten una imagen de transparencia en su gestión y de calidad en sus funciones.

- ✓ **Eficiencia:** Es la mejor utilización social y económica de los recursos administrativos técnicos y financieros disponibles para que los beneficios a los cuales da derecho la seguridad social sean prestados en forma, adecuada, oportuna y suficiente.

- ✓ **Universalidad:** Es la garantía de la protección para todas las personas, sin ninguna discriminación, en todas las etapas de la vida.

VALORES

El Hospital Local de Aguachica, adopta los siguientes valores del Servicio Público – Código de Integridad expedido por el Departamento Administrativo de la Función Pública:

- **Honestidad:** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.
- **Respeto:** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.
- **Compromiso:** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.
- **Diligencia:** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia, para así optimizar el uso de los recursos del Estado.
- **Justicia:** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

LEMA

"Salud, Calidad y Servicio con Excelencia"

OBJETIVOS ESTRATEGICOS

1. Fortalecer la prestación de los servicios de salud, mediante la implementación de un modelo de gestión integral basado en la evidencia, en la gestión del conocimiento y en la innovación, que garantice una atención humanizada,

oportuna, segura, digna y costo-efectiva para todos los usuarios del Hospital Local de Aguachica, E.S.E.

2. Garantizar una Infraestructura Hospitalaria adecuada, que permita ofertar servicios competitivos, dignos y seguros para toda la población usuaria.

3. Diseñar e Implementar un Sistema Integrado de Gestión de Calidad, basado en una transformación cultural, que oriente a la institución a la obtención de altos estándares de calidad, al reconocimiento en el medio, a la satisfacción y fidelización de sus usuarios y familias, y al mejoramiento y aprendizaje organizacional.

4. Ayudar a la formación de competencias del talento humano del Hospital Local de Aguachica E.S.E., a través de la creación de un ambiente laboral de mutua confianza, con base en relaciones de trabajo respetuosas, claras, equitativas y justas, el desarrollo de un modelo de gestión por competencias y la gestión del conocimiento, que con lleven al desarrollo integral de las personas y la productividad de la empresa.

5. Desarrollar la tecnología en el Hospital Local de Aguachica E.S.E., de manera que garantice la atención de salud con seguridad mediante la actualización, mantenimiento, reposición de equipos adquisición y la estandarización del conocimiento institucional basada en la adopción de tecnología adecuada.

6. Consolidar y mantener el sistema de información modular integral en los diferentes procesos estratégicos, administrativos, financieros y asistenciales, a través de una infraestructura tecnológica innovadora y adecuada que permita a todo el personal

del Hospital Local de Aguachica E.S.E., manejar las TICS, para la gestión eficiente de los procesos y la toma asertiva y oportuna de decisiones.

7. Generar rentabilidad económica y social mediante la implementación de procesos eficientes, que permitan mejorar la productividad y venta de servicios, adecuada contención de los costos, reducción de gastos y manejo adecuado de los recursos.

8. Diseñar e implementar el modelo integral Docencia-servicio permitiendo brindar apoyo a los convenios institucionales.

POLITICAS INSTITUCIONALES

POLITICA INSTITUCIONAL

El Hospital Local De Aguachica, es una empresa social del estado cuyo compromiso está fundamentado en una organización ágil, con personal calificado, garantizando una atención integral y oportuna al usuario, sustentando su accionar en los principios de mejoramiento continuo, colaboración, oportunidad, pertinencia, eficacia, austeridad, universalidad, en el tratamiento respaldando sus servicios en la estabilidad financiera que nos permite ser una entidad competitiva y beneficiar así a nuestros usuarios; igualmente comprometidos con el cumplimiento de las directrices legales y reglamentarias enmarcadas en la política del mejoramiento continuo de nuestros procesos, infraestructura, y desarrollo del talento humano, que nos permita lograr una organización sólida y posicionada en la comunidad, siendo reconocida por beneficio social.

POLITICAS DE CALIDAD

La política de calidad del Hospital Local de Aguachica E.S.E., se fundamenta en mejorar continuamente la calidad de la atención a los usuarios y su familia, a través de una Concepción positiva de la Salud, la Participación, la Autonomía, la Implementación de estrategias de Atención Primaria en Salud y el Fortalecimiento de las Competencias del Talento Humano; garantizando el cumplimiento del Sistema Obligatorio de la Garantía de la calidad con una atención en salud con oportunidad, continuidad, eficiencia, seguridad en nuestros servicios centrado en los usuarios y su familia.

POLITICA DE SEGURIDAD DEL PACIENTE

El HOSPITAL LOCAL DE AGUACHICA E.S.E., se compromete en brindar, generar, y mantener un entorno seguro y disponer de recursos para la identificación, prevención y minimización de riesgos, a través de la implementación de programas de vigilancia epidemiológica, cultura de limpieza y desinfección, rondas de seguridad, capacitación continua al personal asistencial y administrativo, mantenimiento de equipos e instalaciones, participación activa en los programa de Reactivo vigilancia, Tecnovigilancia y Farmacovigilancia, seguimiento de los eventos adversos; en un sistema integrado que brinden seguridad al paciente y su familia.

La política de seguridad del Paciente, se fundamenta en implementar estrategias de seguridad en la prestación del servicio de salud, descrito en el Programa de Seguridad del Paciente donde se detalla el procedimiento para identificar, prevenir y reducir los riesgos que se generen durante la atención del usuario, brindando un entorno seguro que garantizan el mejoramiento continuo y la consolidación de la cultura organizacional de la seguridad del paciente.

POLITICA DE HUMANIZACIÓN DE LOS SERVICIOS DE SALUD

La política de Humanización de los servicios de salud del Hospital Local de Aguachica E.S.E, se fundamenta en la interacción del equipo de salud con los pacientes y familia desde una perspectiva integral, comprometiéndose en ofrecer un trato humanizado, respetuoso, digno, confidencial y con garantía de la privacidad durante la atención de los usuarios y su familias, a través de la sensibilización, divulgación y fortalecimiento del conocimiento de los funcionarios y colaboradores de los derechos y deberes de los usuarios, campañas de condiciones de silencio, trato humanizado; con el fin de prestar un servicio de calidad, con atención humanizada, oportuna y efectiva, que responda a las necesidades y expectativas físicas, mentales y sociales del usuario.

Garantizar desde la alta dirección la interacción del equipo de salud con los usuarios y familias desde una perspectiva integral, teniendo en cuenta para ello aspectos culturales, de comunicación, de ambiente físico y tecnológico, de accesibilidad, de acompañamiento espiritual, atención cortés y respetuosa a los usuarios familias y compañeros de trabajo, entre otros aspectos, de tal manera que el paciente y su familia tengan la posibilidad de sentir y vivenciar la dimensión de la humanización.

POLITICA DE ATENCIÓN PREFERENCIAL

El Hospital Local de Aguachica, E.S.E, se encuentra comprometida en ofrecer una atención integral en salud, por lo cual establece la Política de atención preferencial para la población de especial Protección, según lineamientos de la ley 1751 de febrero 16 de 2015, especialmente lo estipulado en el artículo 11. Con el fin de generar estrategias para garantizar que los usuarios y sus familias reciban atención humanizada,

accesible, oportuna, eficiente y con principios de objetividad y buen trato, teniendo en cuenta las condiciones de salud y vulnerabilidad de los usuarios.

LINEAMIENTOS ESTRATÉGICOS DE LA POLÍTICA

Las condiciones de vulnerabilidad tenidas en cuenta en el Hospital Local de Aguachica, E.S.E, para la priorización de la atención de los usuarios y su familia, son:

- Atención de infantes menores de un año
- Atención de mujeres gestantes
- Atención de adultos mayores de 60 años
- Atención de usuarios con algún tipo de discapacidad.

Es responsabilidad de cada funcionario valorar las condiciones especiales de cada paciente que merecen ser tenidas en cuenta para la priorización de su atención y explicar a los otros usuarios las condiciones de vulnerabilidad del paciente que se tomaron en cuenta para la priorización del servicio.

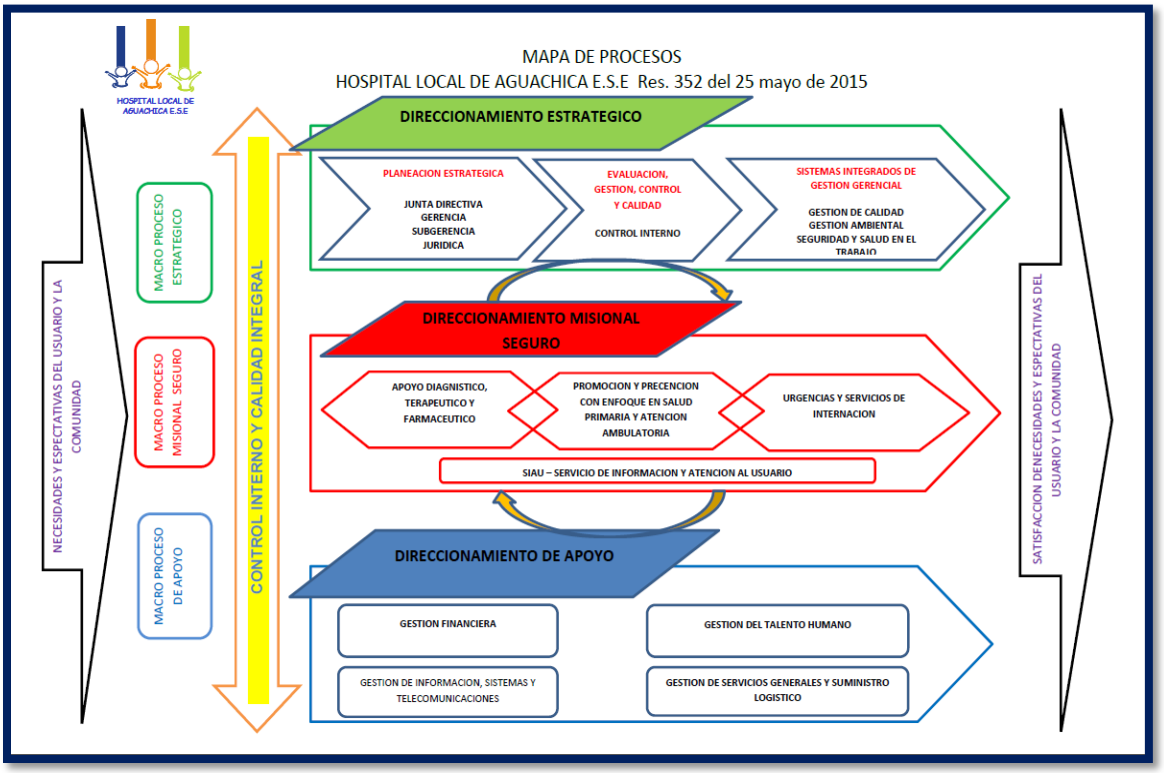
El Hospital Local de Aguachica, E.S.E, cuenta con una ventanilla para la atención preferencia de nuestros usuarios, teniendo en cuenta los criterios de priorización adoptados por la ESE.

Cuando las condiciones del usuario lo requieran, el personal de vigilancia estará atento para proveer los medios necesarios (camilla o silla de ruedas) para su desplazamiento dentro de la institución. De igual manera se garantiza a los pacientes discapacitados los medios y ayuda para el traslado o movilización entre los servicios y pisos del hospital.

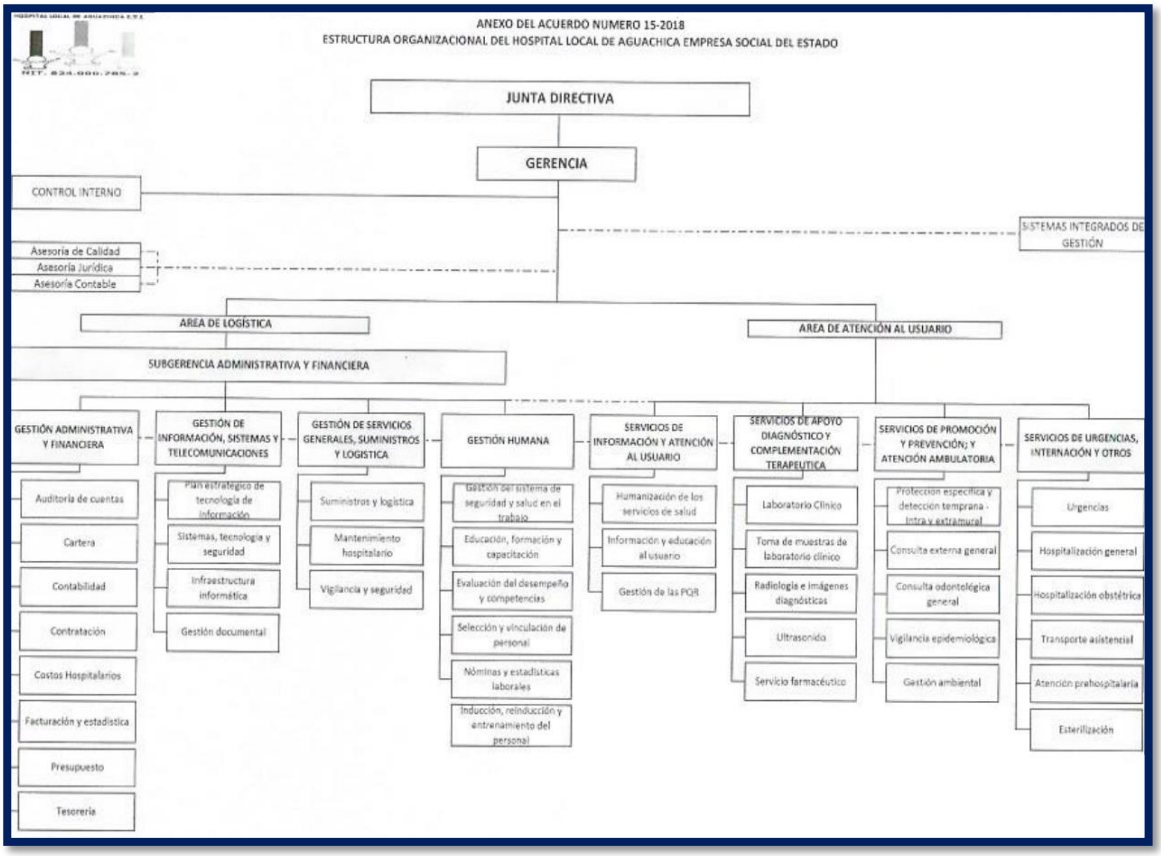
Esta política se ha desarrollado, para efectos de su implementación, por cada uno de los servicios de la institución. En la medida en que este lineamiento hace parte del direccionamiento estratégico de la ESE, se considera de obligatoria aplicación en forma permanente en toda la institución como parte del buen trato y humanización a los usuarios y sus familias.

ESTRUCTURA ORGANIZACIONAL

MAPA DE PROCESOS HOSPITAL LOCAL DE AGUACHICA E.S.E.



ESTRUCTURA DE ÁREAS Y UNIDADES FUNCIONALES



LEVANTAMIENTO DE INFORMACIÓN

La Gerencia del Hospital Local de Aguachica ESE, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la ESE, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la ESE

- Garantizar la continuidad del negocio frente a incidentes.

- La ESE ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la ESE:

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros.**

- La ESE **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- La ESE **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La ESE **protegerá su información** de las amenazas originadas por parte **del personal.**

- La ESE **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos.**

- La ESE **controlará la operación** de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La ESE **implementará control de acceso** a la información, sistemas y recursos de red.

- La ESE garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La ESE garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- La ESE **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La ESE garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

POLÍTICAS

Las políticas que se presentarán a continuación se conforman con una misma estructura: objetivo, aplicabilidad y directrices. La finalidad de estas políticas es que sirvan como herramientas para le entidad no solamente como parámetros de trabajo sino como mecanismos de sensibilización respecto a la seguridad de la información a los usuarios de la ESE Hospital Local De Aguachica, para que así los diferentes procesos de interacción se logren de forma segura, idónea y eficaz.

Política general de seguridad de la información			
Objetivo	Establecer los requisitos generales y necesarios que permitan dar seguridad a la información de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus bienes o servicios informáticos

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

1. Supervisar el ciclo de vida las políticas de seguridad, es decir; definir, implementar, revisar, auditar y actualizar, las políticas de acuerdo a la implementación de esta y la actualización normativa relacionada, así como las necesidades que presenten los usuarios de la entidad
2. Debido a que la entidad cuenta con un área de tecnologías, el asesor en tecnologías de la entidad junto con los responsables de cada servicio deben supervisar y seleccionar los bienes y/o servicios tecnológicos que proyecte adquirir la institución

Organización de la seguridad de la información			
Objetivo	Establecer el comité directivo de la seguridad de la información	**Aplicabilidad**	Todos los funcionarios de los diferentes niveles jerárquicos

Directrices

Fecha de inicio de vigencia: 30-012021
Política autorizada por: Gerencia

1. El comité directivo se conforma por
    a. Gerente
    b. Subdirector administrativo
    c. Subdirector científico
    d. Jefe
    e. Control Interno
    f. Almacenista
    g. Funcionario con responsabilidad en los temas de TIC
2. El comité debe velar por el mejoramiento continuo de los programas o las distintas actividades que se realizarán en este comité
3. Verificar el avance de los distintos proyectos relacionados con esta política
4. Revisar el documento de la política de seguridad
5. Velar por el cumplimiento de las políticas establecidas en este documento

Política de gestión de activos			
Objetivo	Indicar los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de información	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus activos de información

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

6. Se realizará al menos dos veces en el año procesos de identificación y/o actualización del inventario de activos de información por cada una de las dependencias en las cuales los secretarios de despacho serán los responsables de dichos activos de información.
7. Todo activo de información será clasificado de acuerdo a la criticidad, sensibilidad y reserva establecida por la entidad conforme a las leyes como Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015.
8. Los activos de información se deben etiquetar y/o rotular bajo la responsabilidad de cada uno de los secretarios de despacho con el acompañamiento de personal experto.
9. Los funcionarios, contratistas y/o terceros deben realizar la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.
10. Con relación a los medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, los cuales serán autorizados para compartir información autorizada con personal externo a la entidad, siempre y cuando el líder del área de tecnologías y seguridad de la información lo autorice
11. Es obligatorio realizar de forma segura y correcta la eliminación, retiro, traslado o re uso cuando no se requieran los activos de información. Por lo cual es relevante realizar backups los cuales se envíen el acceso o borrado no autorizado.

Política de control de acceso			
Objetivo	Determinar la protección, límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información.	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus activos de información

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

12. El acceso a redes, aplicaciones y/o sistemas de información de la entidad se debe hacer mediante usuarios y contraseñas, y asignadas a cada funcionario el cual es responsable del uso de estas
13. La gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios de los usuarios asignados será administrada por el encargado de TI de la entidad
14. La calidad de las contraseñas constará de al menos 8 caracteres las cuales contendrá caracteres alfa numéricos y especiales.

Política de no repudio			
Objetivo	Evitar acciones de repudio por parte de los usuarios	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus activos de información

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

15. Realizar seguimiento a la creación, origen, recepción y entrega de información
16. Tener logs de registro de las acciones realizadas por los usuarios, la cual será informada a los usuarios
17. Realizar auditorías continuas, como procedimiento para asegurarse que las partes implicadas se nieguen haber realizado una acción
18. Los servicios de intercambio electrónico de información son garantía de no repudio

Política clasificación de la información			
Objetivo	Brindar un nivel de protección apropiado a la información que produce o hace uso la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y la información que estos generen o hagan uso de la entidad

Directrices

Fecha de inicio de vigencia: 30-01-202
Política autorizada por: Gerencia

1. En la entidad se considera como información:
    a. Comunicados o mensajes que son transmitidos de forma oral ya sea personalmente o por medios electrónicos como llamadas de voz, video llamadas entre otras
    b. Comunicados o mensajes que son transmitidos de forma escrita ya sea por medios electrónicos como medios magnéticos, físicos, herramientas de mensajería, entre otros.
    c. Formularios, encuestas y otros mecanismos de captura de información propios o de terceros, ya sea por mecanismos virtuales o físicos

d. Información almacenada o generada en los equipos, sistemas o servicios informáticos, medios magnéticos/electrónicos y/o medios físicos
2. Es responsabilidad del usuario identificar los posibles riesgos a los que puede ser expuesta la información que utiliza ya que esta puede ser copiada, divulgada, alterada o eliminada ya sea de forma física o digital a manos de funcionarios o personal externo de la entidad
3. El funcionario debe seguir los lineamientos de los activos de información de la entidad para lograr la identificación y administración óptima de estos

Política seguridad en el papel del talento humano			
Objetivo	Reducir el riesgo de uso no adecuado de la información por parte de los usuarios de los bienes y servicios informáticos de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y sus bienes o servicios informáticos

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

1. Los usuarios deben entender las responsabilidades de sus cargos o funciones con las políticas de seguridad de la información de la entidad para así disminuir el riesgo del uso no adecuado, pérdida, hurto, fraude o filtración de la información en los bienes y servicios informáticos utilizados de la entidad
2. Se recomienda al usuario crear una cuenta con su correo electrónico institucional en herramientas de servicio de almacenamiento en la nube tales como Dropbox, Drive u Outlook, para que pueda tener un respaldo de se seguridad de su información en caso de daños al equipo. Sobre esta cuenta tendrá conocimiento la administración municipal y las oficinas encargas del área de TI
3. Los programas que se instalarán en las estaciones de trabajo (equipos de cómputo y Smartphone) deben cumplir con dos características: 1. Licenciandos (legales) y 2. Autorizados por las personas encargadas de Tecnologías de Información en la entidad, no se permite el uso de software que no cumpla con esas condiciones
4. Las herramientas software de la entidad deben tener su respectiva licencia y cumplir con lo acordado por los derechos de autor
5. Las herramientas instaladas sin autorización del área de TI en la entidad deben ser eliminadas ya que esto expone a posibles ataques informáticos en la entidad
6. Buscando agilidad y seguridad de la información, todo dispositivo de almacenamiento externo al equipo de trabajo de cómputo tales como memorias Flash USB, DVD, CD, Dispositivos móviles, entre otros, serán analizados automáticamente por una plataforma

Política seguridad en el papel del talento humano
de antivirus, a menos que el Sistema Operativo en uso represente una seguridad tal que no necesite la instalación de software antivirus 7. Las herramientas software instaladas en los equipos de cómputo de la entidad son propiedad de esta. En el caso que sean aplicativos de entidades de orden nacional estos pertenecerán a sus distribuidores y la entidad tendrá tan solo derechos de uso, por lo tanto las licencias o las mismas herramientas software no pueden ser copiadas 8. La entidad puede realizar auditorías anunciadas y no anunciadas con la finalidad de mantener la integridad institucional con el fin de identificar copias no autorizadas de programas o herramientas en los equipos de cómputo en la entidad 9. Los bienes y servicios tecnológicos asignados a cada usuario de la entidad son responsabilidad de dicho usuario 10. Debido a la responsabilidad de cada usuario sobre los bienes y servicios informáticos asignados este debe abstenerse de almacenar en ellos información que no sea de carácter institucional, de acuerdo a los parámetros de activos de información 11. La información no autorizada para su divulgación por parte de los usuarios de la entidad acarreará responsabilidades disciplinarias y legales 12. Los bienes y servicios tecnológicos de la entidad deben ser utilizados únicamente para el propósito que estos fueron adquiridos 13. Antes la presencia de eventos que el usuario considere que pueden debilitar o comprometer la seguridad de la información en la entidad, se debe reportar a las personas encargadas del área de TI de la entidad 14. Con el apoyo de los funcionarios de primer nivel se socializarán una serie de lineamientos a tener en cuenta al momento de compartir información reservada de la entidad como contraseñas de acceso a diferentes servicios informáticos y otra información de carácter confidencial a través de medios de comunicación virtuales o presenciales tales como: llamadas telefónicas, aplicaciones de mensajería, o conversaciones presenciales 15. Para compartir información entre una usuario y otro es mejor utilizar medios de comunicación auditados como el correo electrónico o la intranet

Políticas para funcionarios y contratistas del Área de Tecnologías y Sistemas de Información			
Objetivo	Establecer los lineamientos que garanticen la seguridad de la información de la entidad por parte de los funcionarios y contratistas de TI	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. El personal del área de TI no debe dar a conocer contraseñas de acceso a terceros sin previa autorización de la persona líder del Área de TI 2. Los usuarios y claves de acceso de los administradores de sistemas y del personal del Área de TI son información de uso personal e intransferible 3. El Área de TI debe emplear el uso de contraseñas de alto nivel de complejidad, autenticación en dos vías para el acceso a servicios TI que administren usuarios o herramientas en la entidad			

Políticas para funcionarios y contratistas del Área de Tecnologías y Sistemas de Información
4. La información de procedimientos, seriales, software entre otros deben mantenerse bajo custodia para evitar el acceso a personas no autorizadas 5. Cuando se realice el cambio o retiro de equipos de los funcionarios o usuarios de la entidad, es necesario seguir políticas de saneamiento, es decir, prácticas que mejoren la eliminación de la información contenida, a través de un formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos 6. El personal de TI encargado de realizar instalaciones de software en los equipos de cómputo de la entidad, instalará herramientas licenciadas y/o legales autorizados 7. Sin la autorización correspondiente los encargados del Área de TI no debe otorgar permisos especiales a los usuarios de los diferentes bienes o servicios tecnológicos de la entidad 8. Los encargados del Área de TI no utilizará la información para fines comerciales o diferentes al ejercicio de sus funciones 9. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro. 10. Todo bien o servicio informático y sus medios, deben ser únicamente instalados en los equipos y servidores de la entidad, donde a su vez se deben hacer copias de seguridad de acuerdo con las políticas del proveedor y de la entidad 11. Deben ser bloqueados los protocolos y servicios que no se requieren en los equipos de cómputo de la entidad, a menos que sean solicitados y aprobados oficialmente por la entidad a través del Área de TI. 12. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado

Políticas para el/la Administrador del sitio web			
Objetivo	Mantener la integridad del sitio Web Institucional, software o aplicativos e información contenida	**Aplicabilidad**	Las personas encargadas de la actualización y soporte del sitio web de la entidad
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Las personas encargadas de la actualización y soporte del sitio web de la entidad deben apegarse a la seguir la Política Editorial y Actualización de Contenidos Web, así como los lineamientos de la estrategia Gobierno en Línea 2. Las claves de acceso al administrador del Sitio web institucional de la entidad son estrictamente confidenciales, personales e intransferibles		

Política de disponibilidad de información, medios y equipos			
Objetivo	Disponer de un funcionamiento óptimo de los equipos, información y distintos medios tecnológicos	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

	ante posibles fallas o desastres en la entidad		
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Los medios y equipos donde se almacene, procese o comparta información, deben contar con lineamientos de protección física y lógica 2. Realizar monitoreo sobre el estado del funcionamiento de los medios y equipos de información 3. Realizar mantenimientos preventivos y correctivos pertinentes			

Política de integridad, respaldo y restauración de información			
Objetivo	Establecer mecanismos de respaldo adecuados para conservar la información y software antes posibles fallas	**Aplicabilidad**	Personal encargado de administrar los bienes y servicios de TI en la entidad
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Almacenar de forma regular la información de los equipos en medios magnéticos como CD, DVD, Cartucho, Cinta, etc... 2. El funcionario o asesor encargado de coordinar el uso de bienes y servicios de TI debe establecer la frecuencia con la cual se realicen respaldo a estos activos de información 3. Las copias de información importantes deben almacenarse en un lugar que garantice la integridad de la información almacenada 4. La finalidad de guardar copias de respaldo es que se utilizarán únicamente cuando el sistema o área de trabajo deba ser reestablecida debido a daños de hardware o software, o por requerimiento legal 5. Se debe mantener un inventario actualizado de los respaldos realizados a los diferentes equipos o sistemas informáticos			

Política de uso de estaciones de trabajo			
Objetivo	Garantizar la seguridad y buen uso de las estaciones de trabajo de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia			

Política de uso de estaciones de trabajo
1. La instalación de software en los computadores de las dependencias es una función que puede realizar solamente el Área de TI de la entidad, además de dispondrá en una lista actualizada del software autorizado para instalar en los computadores 2. La unidad de almacenamiento de cada estación de trabajo deberá estar dividida en al menos dos discos virtuales (C: y D:) donde el disco C: contendrá el sistema operativo y software para las labores del funcionario, mientras que el disco D: contendrá los archivos o información generada por el funcionario, esto con el fin de mejorar el nivel de integridad de la información, a menos que se cuente un Sistema Operativo Linux, el cual garantiza la integridad de la información independiente de sus archivos de S.O 3. Las terminales de trabajo (computadores de escritorio) no pueden salir de la entidad o ser llevadas de una oficina a otra a menos que lo autorice y supervise el Área de TI, en el caso de los equipos portátiles que pertenezcan a la entidad pueden ser transportados libremente dentro la entidad siempre y cuando por la persona responsable del equipo, pero no deben salir de la institución, a menos que el Área de TI lo autorice, además debe llevarse un registro de salida y entrada de equipos debidamente firmado por cada funcionario 4. Cuando un usuario quiera prestar un equipo que está bajo su responsabilidad a otro usuario dentro la entidad debe solicitar autorización al Área de TI y dejar registro del préstamo realizado donde los dos usuarios firmen la entrega y recibido del mismo

Política de uso Internet			
Objetivo	Definir los lineamientos que establezcan una navegación segura y uso adecuado de la red de la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. La navegación en internet debe realizarse con propósitos labores o que busquen mejorar el rendimiento laboral y personal de los usuarios de la entidad 2. No es permitida la navegación en sitios con contenidos contrarios a la ley o políticas de la entidad, los cuales puedan presentar riesgos tales como: pornografía, terrorismo, hacktivismo, segregación o discriminación racial, entre otros que puedan atentar con la integridad de la entidad y su misión y visión 3. En caso de acceder a este tipo de contenidos con fines de investigación o seguridad, se debe contar con la autorización del Área de TI 4. La descarga de archivos de internet debe ser con fines laborales y de manera coherente al uso común de la misma, es decir no se deben realizar con regularidad descargas que afecten el ancho de banda de la red ya que limita el uso de la misma a los demás funcionarios en la entidad, en caso de realizar descargas de mayores a 400 Mbs se recomienda hacerlas en horarios no laborables, dejando que el equipo realice el proceso de forma automática		

Política de mensajería instantánea y redes sociales			
Objetivo	Definir lineamientos para el uso de servicios de mensajería instantánea y redes sociales para usuario autorizados	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios **autorizados** que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

1. El uso de mensajería instantánea y acceso a redes sociales por medios de los bienes y/o servicios informáticos de la entidad debe ser realizado únicamente por los **usuarios autorizados** por el Área de TI
2. Todo usuario que no esté autorizado para hacer uso de redes sociales y herramientas de mensajería instantánea con los bienes y/o servicios informáticos de la entidad debe abstenerse de hacer uso de estas
3. No se permite el envío de mensajes con contenido que atente con la integridad de la comunidad en general o instituciones al igual se prohíbe material que pueda contener o llevar a lugares con código malicioso
4. La información que se publique en redes sociales o por medio de herramientas de mensajería instantánea a nombre personal es considerada fuera del alcance del Área de TI de la entidad y la entidad misma, y por lo tanto su fidelidad, coherencia, confiabilidad, integridad y disponibilidad y los potenciales daños o perjurios causados o que puedan causar son responsabilidad explicita de la persona que haya producido esta tipo de contenido

Política de uso de impresoras y servicio de impresión			
Objetivo	Fomentar una correcta operación e integridad de las impresoras y servicios de impresión en la entidad	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI

Directrices

Fecha de inicio de vigencia: 31-01-2021
Política autorizada por: Gerencia

1. El uso de los dispositivos de impresión deben alinearse principalmente a la política de cero papel de la entidad
2. Los documentos que se impriman en la entidad deben ser de carácter institucional y laboral
3. El usuario debe dar un correcto uso a los equipos de impresión que están a su cargo para evitar el posible daño de estos

Política de uso de impresoras y servicio de impresión
4. Se recomienda a los usuarios no realizar labores de reparación o mantenimiento de las impresoras, específicamente en sus características de hardware, en caso de presentarse alguna falla debe contactarse el área de TI de la entidad

Política de uso de puntos de acceso a las redes LAN y Wi-fi			
Objetivo	Coordinar un uso correcto de los puntos de acceso a la red, intranet e internet	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Los equipos de trabajo de la entidad se deben conectar a la red por medio de puntos LAN, red cableada, esto con el propósito de estabilidad y seguridad de la información 2. Los usuarios como contratistas, invitados y entre otros que no son funcionarios de planta en la entidad, deben conectar sus terminales a las redes wi-fi puestas a disposición en la entidad. El acceso a estas redes deben ser autorizadas y configuradas por el Área de TI 3. La activación, gestión y uso de los punto de red en la entidad es responsabilidad el Área de TI			

Política de seguridad de los Equipos			
Objetivo	Asegurar la idoneidad de la información almacenada en los equipos	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. El suministro de energía de los equipos en caso de no ser regulada, debe contar al menos cada equipo con un dispositivo tal como un estabilizador y en el caso que sea posible una UPS 2. El cableado debe estar marcado para identificar los elementos conectados y evitar desconexiones erróneas 3. Es necesario realizar soporte y mantenimiento a los equipos, por lo tanto es recomendable tener contratos de soporte tanto preventivo como correctivo 4. Es necesario llevar registro de las acciones de soporte y mantenimiento realizadas a los equipos de la entidad 5. En caso que un equipo deba ser retirado de la entidad y trasladado a laboratorios u organizaciones de soporte y mantenimiento de equipos informáticos es necesaria la autorización y registro de la salida y enredada de estos			

Política de seguridad de los Equipos
6. El ingreso y retiro de todo activo de información en la entidad debe ser registrado y autorizado por el Área de TI

Política de escritorio y pantalla limpia			
Objetivo	Definir los lineamientos para reducir el riesgo de acceso no autorizado, pérdida y daño de información	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, Organizaciones y demás potenciales usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. El escritorio del equipo de trabajo del usuario debe estar libre de información para que esta no pueda ser copiada o eliminada fácilmente por otros usuarios o terceros sin autorización, además de facilitar el soporte del terminal 2. La pantalla se debe bloquear toda vez que el usuario no esté en su estación de trabajo, para lo cual es recomendable establecer contraseña al usuario con el que se inicia sesión 3. Al imprimir documentos de tipo confidencial, estos deben ser retirados inmediatamente de la impresora			

Política de uso del correo electrónico			
Objetivo	Definir lineamientos para asegurar la protección de la información de la entidad en el uso de correo electrónico	**Aplicabilidad**	Todos los funcionarios, Directivos, Contratistas, y usuarios que tengan relación con la entidad y el uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Los usuarios de correo electrónico corporativo (institucional) son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información 2. El acceso al correo electrónico se realizará de forma local en el equipo asignado a cada funcionario, a través de herramientas administradoras de correo electrónico instaladas en el equipo de trabajo 3. La finalidad del uso de correo electrónico es de carácter operativo, laboral e institucional 4. No se debe utilizar este correo para fines personales o compartir información personal 5. No está permitido el envío de cadenas o correos masivos que no sean de tipo laboral 6. Se debe procurar evitar el envío de correos electrónicos con un peso superior a las 20 MB 7. No está permitido el envío de correos que atenten contra la integridad y dignidad de las personas o que puedan dañar su buen nombre			

Política de uso del correo electrónico
8. Cuando un funcionario se retire de su cargo el correo continuará vigente y entrará en funcionamiento al nuevo funcionario asignado 9. El tamaño del correo electrónico está en función de la capacidad del equipo de trabajo donde este se encuentre instalado 10. Se creó una cuenta de correo electrónico en la web donde se reenviarán todos los correos recibidos en las cuentas institucionales que servirá como Backup 11. Las cuentas de correo no son propiedad del funcionario o usuario, son propiedad del sistema de administración web el cual presta el servicio en la entidad 12. El usuario es responsable de la información y archivos adjuntos que se envían desde la cuenta de correo asignada 13. Todo mensaje que el usuario considere sospechoso debe ser reenviado a la cuenta de correo para realizar su análisis, además este correo sospechoso debe ser eliminado y no abrir ningún enlace o archivo adjunto contenido en el mismo

Política de uso de la red intranet			
Objetivo	Definir lineamientos para hacer buen uso de la red intranet de la entidad	**Aplicabilidad**	Todos los funcionarios que hagan uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Los usuarios conectados a la red interna (intranet) por medio de conexión cableada serán los autorizados para hacer uso de esta 2.La intranet les permitirá compartir archivos entre funcionarios con una velocidad de 100Mb/s lo que representaría una horro en el ancho de banda de internet 3. Además, podrán realizar Backups en el servidor central, con un tamaño máximo de 10Gb por usuario 4. No se permite el uso de la intranet para realizar tareas personales o compartir archivos que no estén relacionados con las labores o funciones de la institución			

Política de uso servicio de mensajería Empathy			
Objetivo	Definir lineamientos para hacer buen uso del servicio de mensajería	**Aplicabilidad**	Todos los funcionarios que hagan uso específico de herramientas o servicios de TI
Directrices			
Fecha de inicio de vigencia: 30-01-2021 **Política autorizada por:** Gerencia 1. Este servicio tiene con finalidad facilitar la comunicación con fines laborales entre funcionarios 2. Se recomienda hacer un buen uso del lenguaje, respetando la integridad de los demás funcionarios 3. Este servicio será auditado, así que está prohibido eliminar las conversaciones entre funcionarios			

Política de privacidad y confidencialidad			
Objetivo	Establecer los parámetros de protección de datos personales que deben ser aplicados, conforme en la normatividad vigente	**Aplicabilidad**	Sistemas de información y otros medios de captura de información del usuario, ciudadano o funcionario que haga uso de los servicios de la entidad

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

1. Ámbito de aplicación: La Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
2. Excepción de la aplicación: Bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Las que tengan por finalidad la seguridad y defensa nacional prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo. Las que tengan como fin y contengan información de inteligencia y contrainteligencia. Las que contengan información periodística y otros contenidos editoriales. Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.
3. Principio del tratamiento de datos personales: Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente. Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular. Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos. Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento. Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente. Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información
5. Derechos de los titulares: Conocer, actualizar y rectificar sus datos personales. Solicitar la prueba de su autorización para el tratamiento de sus datos personales. Ser informado respecto del uso que se le da a sus datos personales. Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización. Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.
6. Para obtener autorización del titular para el tratamiento de sus datos personales, debe presentar carta de autorización debidamente certificada por notaria municipal. Los casos en los cuales no se requiere autorización del titular están relacionados en el punto 2

7. Los deberes de los responsables de y/o encargados del tratamiento de datos son: velar por la integridad de la información, preservar la confidencialidad de los datos y garantizar de forma organizada y coherente la captura de datos.
8. Los sistemas de información deben garantizar mediante controles criptográficos la confidencialidad y autenticidad de la información capturada o generada, mediante estándares de Algoritmo Hash Seguro.

Política de registro y auditoria			
Objetivo	Velar por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información	**Aplicabilidad**	En los activos de información de la entidad

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

1.La oficina de Control Interno, es responsable de llevar a cabo las auditorias periódicas a los sistemas y actividades relacionadas a la gestión de activos de información y a su vez informar los resultados obtenidos
2. Se debe almacenar los registros de las copias de seguridad en la base de datos correspondiente y dar correcto funcionamiento de las mismas. Estos registros deben incluir toda la información registro y monitoreo de eventos de seguridad
3. Se debe velar porque las auditorias sean realizas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad
4. Se debe dar garantía a la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad, así como recomendar las deficiencias detectadas
5. Se determina una revisión periódica de al menos cada seis meses de los niveles de riesgos a los cuales está expuesta la Entidad, las cuales están alineadas a los objetivos estratégicos y gestión de procesos de la Entidad

Política de gestión de incidentes			
Objetivo	Documentar la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.	**Aplicabilidad**	Todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

Directrices

Fecha de inicio de vigencia: 30-01-2021
Política autorizada por: Gerencia

1.Reportar los eventos, incidentes y vulnerabilidades establecidas en el plan de tratamientos de riesgos al comité de seguridad de información de la entidad por medio de reportes oficiales
2. Los responsables de gestionar los eventos son las personas encargadas de velar por la seguridad e integridad de la información en la entidad

3. Se evaluarán periódicamente los logros de reportes de incidentes de los sistemas de información y se construirá un informe oficial con la explicación de los incidentes reportados
4. Realizar documentación oficial sobre el esquema de gestión y los procedimientos
5. El equipo encargado de manejar los incidentes será el liderado por el área de TI y seguridad de la información de la entidad

Política capacitación y sensibilización en seguridad de la información			
Objetivo	Formar al personal de la entidad en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano	**Aplicabilidad**	Todos los funcionarios y contratistas de la entidad
Directrices			
Fecha de inicio de vigencia:30-01-2021 **Política autorizada por:** Gerencia 1.Destinar recursos suficientes para desarrollar los programas de formación 2. Capacitar a los funcionarios de la entidad y contratistas relacionados con temas específicos de la seguridad e integridad de la información 3. Es obligatoria la asistencia a los eventos de capacitación por parte de los funcionarios y contratistas 4. Realizar revisión periódica de resultados de capacitaciones para mejoramiento de los procesos 5. Definir roles y responsabilidades que quienes diseñaran los programas y a quienes los comunicarán 6. Realizar una documentación detallada sobre los planes de estudio y desarrollo de los programas 7. Establecer compromisos y obligaciones por parte del personal capacitado		

PROCEDIMIENTOS

Los procedimientos son la descripción de la forma detalladas sobre las actividades necesarias en la realización de un proceso, los procedimientos listados siguen las normas de los lineamientos de acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001.

- Procedimiento de control de registros
- Procedimiento de auditoría interna
- Procedimiento de acción correctiva
- Procedimiento de acción preventiva
- Procedimiento de revisión del Manual de la Política de Seguridad

PROCESO DISCIPLINARIO

La oficina de Gestion de información Sistemas y Telecomunicaciones adopta en su modelo de procesos, el proceso de Seguridad y Privacidad de la Información en el nivel estratégico que permitirá garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la ESE, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

A continuación, se presenta el listado de acciones que pueden llevar al usuario a cometer faltas de tipo disciplinario y a su vez violar los procedimientos de seguridad de la información:

- No participar en la socialización de los lineamientos y acuerdos de confidencialidad sobre el uso y entrega de los activos de información.
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al Área de TI de la entidad.

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
- Dejar información pública reservada, en carpetas compartidas
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios.
- Dejar los computadores encendidos en horas no laborables, a menos que el Área de TI solicite lo contrario.
- Permitir que personas ajenas a la entidad, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
- Solicitar cambio de contraseña de un usuario distinto al otorgado al funcionario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (exceptuando el penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.

- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional, tanto de los bienes o servicios informáticos.
- Compartir correos electrónicos no institucionales para recibir o enviar información laboral de la entidad.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación
- Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de TI de la entidad
- Permitir el acceso a particulares o terceros a los servicios o bienes tecnológicos asignados a cada usuario sin la autorización del Área de TI
- Uso de servicios disponibles a través de internet que no estén permitidos por el Área de TI tanto como acceso FTP, Telnet, protocolos y servicios los cuales pueden generar riesgo a la entidad
- Mal uso de los equipos de escritorio o portátiles, teléfonos inteligentes y otros dispositivos entregados a los usuarios para actividades laborales
- Ocultar, destruir, copiar y/o eliminar de la documentación institucional, o destruirla de forma errónea

- Dejar sin supervisión documentación con información pública reservada o clasificada de la institución
- Copiar o almacenar información pública reservada o clasificada, en dispositivos de almacenamiento tales como: memorias flash USB, computadores portátiles, teléfonos, entre otros dispositivos que permitan el almacenamiento de información digital y que no permanezcan en la institución
- Conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la institución, sin la autorización del Área de TI
- Guardar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos
- Uso de los recursos de la institución como servicios, bienes o espacios en redes sociales o medios web, para el beneficio personal del usuario
- Eliminar, dañar, borrar, o programar el borrado de datos informáticos o de un sistema de información de la institución
- Distribuir, enviar, instalar o permitir el ingreso a software malicioso u otros programas de computación de efectos dañinos en los bienes o servicios informáticos de la entidad
- Alterar o corromper datos personales de las bases de datos de la institución
- Suplantar a un usuario en alguno o todos los sistemas tecnológicos de la entidad
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la entidad o permitir que otras personas accedan con el usuario y clave del responsable a éstos

- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la institución a personas no autorizadas
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceder a servicios o bienes informáticos no autorizados de la institución o de terceros
- Llevar a cabo acciones que su propósito o resultado evite o altere los controles de seguridad establecidos en la institución
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización del Área de TI
- Sacar de las instalaciones de la entidad de forma física o virtual, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la entidad, para traslado, reasignación o para disposición final
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la entidad o de alguno de sus funcionarios
- Acceder, almacenar o distribuir pornografía infantil
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de TI de la entidad

- Copiar sin autorización los programas de la entidad, o violar los derechos de autor o acuerdos de licenciamiento

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique	JESUS BALLESTEROS	Documentación actualizada en SIMIG	1-02-23	31-03-23
	Levantamiento Activos de Información	Socializar la metodología de activos de Información.	JESUS BALLESTEROS	Listado de asistencia	01-04-23	30-04-23
		Validar activos de información en el instrumento levantado en la vigencia anterior	ING. TELECOMUNICACIONES	Acta de Reunión	01-05-23	31-05-23

Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
Activos de Información	Levantamiento Activos de Información	Identificar nuevos activos de información en cada dependencia	**ING. TELECOMUNICACIONES**	Informe de los nuevos Activos	01-06-23	30-06-23
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	**ING. TELECOMUNICACIONES**	Correos electrónicos	1-07-23	31-07-23
	Levantamiento Activos de Información	Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	**ING. TELECOMUNICACIONES**	Formato hoja de vida de los equipos	8-ago-23	31-ago-23
		Actualización del inventario de activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	**ING. TELECOMUNICACIONES**	Formato de hoja de vida de equipo con las novedades	01-09-22	31-09-22
	Levantamiento Activos de Información	Consolidar el instrumento de activos de Información.	**ING. TELECOMUNICACIONES**	Consolidado activos de la información MinTIC	3-oct-23	31-oct-23

	Publicación de Activos de Información	Publicar los instrumentos de activos de información consolidado.	**ING. TELECOMUNICACIONES**	Relación de los activos de información de la institución.	01-11-23	30-11-23
	Registros activos de información ley 1712	Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información.	**ING. TELECOMUNICACIONES**	Documento Registro Activos de Información	01-12-23	31-12-23
		Enviar a control de legalidad el instrumento de Registro Activos de información.	**JEFE DE SISTEMAS**	Correo electrónico	01-12-23	31-12-23
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	**Oficina Asesora de Prensa, Oficina de TI**	Correo electrónico con la solicitud	01-12-23	31-12-23
	Reporte Datos Personales	Reportar al Oficial de Protección de Datos personales la información recolectada en el instrumento de activos, correspondiente a bases de datos con datos personales.	**Oficial de Protección de Datos personales**	Consolidado activos de la información publicado	01-12-23	31-12-23
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	**Equipo de Gestión de Riesgos**	Correos electrónicos, Documentación actualizada	01-02-23	30-11-23
	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	**Equipo de Gestión de Riesgos**	Listas de asistencia, Correos electrónicos	01-02-23	31-05-23
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	**Equipo de Gestión de Riesgos**	Correos electrónicos Mapas de riesgos	01-03-23	31-03-23

	Digital y continuidad de la Operación	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	**Equipo de Gestión de Riesgos**	Correos electrónicos Mapas de riesgos	01-03-23	31-03-23
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	**Equipo de Gestión de Riesgos**	Memorandos de aceptación mapas de riesgos	02-05-23	30-06-23
	Publicación	Publicación mapas de riesgos	**Equipo de Gestión de Riesgos**	Mapas de riesgos publicados	1-jun-23	30-jun-23
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de los planes de tratamiento y al seguimiento de la valoración de los riesgos residuales.	**Equipo de Gestión de Riesgos**	Correos electrónicos	01-02-23	31-12-23
	Mejoramiento	Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Equipo de Gestión de Riesgos	Correos electrónicos, Documentación actualizada	1-02-23	30-12-23
Gestión de Incidentes de Seguridad y Privacidad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación cuando se requiera el procedimiento de incidentes de seguridad de la información.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	Documentación actualizada	01-02-23	30-12-23
	Gestionar los incidentes de Seguridad de la Información identificados	Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo a lo establecido en el procedimiento definido	Encargado de la Gestión de Incidentes de Seguridad de la Información.	Correos electrónicos, seguimiento al reporte de incidentes	1-02-23	31-12-23
Planeación	Revisión Manual Políticas de Seguridad de la Información y	Actualizar cuando se requiera los Manuales, Políticas, Resoluciones, documentación del SGSPI y la documentación estratégica del proceso de Seguridad y privacidad de la Información.	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Documentación actualizada en Página Web	01-02-23	23-12-23

	Resolución de Seguridad de la Información	Actualizar el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos.	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Documentación actualizada en SIMIG y Página Web	01-11-23	31-01-24
Protección de datos personales	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial de Seguridad y Privacidad de la Información y Gestor de procesos	Formatos y listados de asistencia	1-02-23	20-dic-22
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Seguridad y Privacidad de la Información	Certificado del registro de BD	01-03-23	31-dic-23

CONTROL DE CAMBIOS

NÚMERO DE VERSIÓN	FECHA			RESPONSABLE	DESCRIPCION
	dd	mm	aaaa		
1.0	26	01	2022	THANIA MILENA OLIVAR QUIN	Elaboración del Plan
1.1	16	01	2023	THANIA MILENA OLIVAR QUIN	Actualización del Plan

REGISTRO DE ELABORACIÓN Y APROBACIÓN DE DOCUMENTO

Elaboró		**Revisó**	**Aprobó**
Nombre	Thania milena olivar		Comité de gestion y desempeño
Cargo	Prof. Univ. Sistemas		
Firma			
Fecha			

BIBLIOGRAFÍA

No hay ninguna fuente en el documento actual.