1. NORMATIVA

- **Ley 527 de 1999** – por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
- **Ley 594 de 2000** – Ley General de Archivos.
- Ley Estatutaria 1266 de 2008 – disposiciones generales del hábeas data (financiera, crediticia, comercial, etc.).
- **Ley 1273 de 2009** – delitos informáticos y protección de los datos y sistemas que usan TIC.
- **Ley 1341 de 2009** – principios y marco regulatorio de las TIC (modificada por Ley 1978 de 2019).
- **Ley 1437 de 2011** – Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Capítulo IV, medios electrónicos y documentos electrónicos).
- **Ley 1581 de 2012** – disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014** – Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- **Ley 1915 de 2018** – reforma a la Ley 23 de 1982 sobre derecho de autor y derechos conexos.
- **Ley 2015 de 2020** – interoperabilidad de la Historia Clínica Electrónica.
- **Decreto 1151 de 2008** – estrategia de Gobierno en Línea.
- **Decreto 235 de 2010** – intercambio de información entre entidades para funciones públicas.
- **Decreto 1377 de 2013** – reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014** – reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 1074 de 2015** – Decreto Único Reglamentario del Sector Comercio, Industria y Turismo (compila D. 1377/2013 y 886/2014).
- **Decreto 1081 de 2015** – Decreto Único Reglamentario de la Presidencia de la República (transparencia y acceso a la información).
- **Decreto 1078 de 2015** – Decreto Único Reglamentario del Sector TIC (Gobierno Digital).
- **Decreto 090 de 2018** – modifica el Registro Nacional de Bases de Datos.
- **Decreto 767 de 2022** – actualiza la Política de Gobierno Digital.
- **Conpes 3995 de 2020** – Política Nacional de Confianza y Seguridad Digital.
- **Circular Única SIC** – Título V Protección de Datos Personales.
- **Circulares Externas SIC 002 y 003 de 2024** – guías de cumplimiento en protección de datos.
- **Manuales y guías de Gobierno Digital** (MinTIC).
- **Resolución 1995 de 1999** – organización, manejo y custodia de la Historia Clínica.
- **Resolución 3100 de 2019** – inscripción y habilitación de prestadores y servicios de salud.
- **Directiva Distrital 005 de 2005** – políticas generales de TIC para entidades del Distrito Capital.
- **ISO/IEC 27001:2022** – Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27002:2022** – Controles de seguridad de la información.
- **ISO/IEC 27005:2018** – Gestión de riesgos de seguridad de la información.

- **ISO/IEC 27701:2019** – Extensión para la gestión de privacidad.
- **ISO/IEC 27017 y 27018** – Controles de seguridad y protección de datos en la nube.

2. ALINEACIÓN CON EL DIRECCIONAMIENTO ESTRATÉGICO

La Política de seguridad digital de la Subred integrada de Servicios de Salud Sur ESE se articula con la Plataforma Estratégica desde el enfoque:

Misión: La Subred Integrada de Servicios de Salud Sur E.S.E., brinda a través de un Modelo basado en la Atención Primaria Social, integral e integrado, servicios de salud enfocados a una gestión de riesgo, con excelencia, humanizada y comprometida con MÁS SALUD Y MÁS BIENESTAR; contando con un talento humano altamente calificado, transparente, comprometido, con vocación de docencia y servicio soportado en una gestión del conocimiento, innovadora e investigativa que contribuye al mejoramiento de las condiciones de vida de la población urbana y rural bajo un enfoque diferencial.

Visión: Consolidarnos en el año 2028, como una Empresa Social del Estado referente a nivel nacional en la Prestación de Servicios de Salud con MÁS Bienestar, con estándares superiores de calidad, líderes en docencia, con avances significativos en investigación, sostenibilidad financiera y ambiental; manteniendo un enfoque incluyente, diferencial y multicultural que promueva la intersectorialidad aportando al mejoramiento de la calidad de vida de nuestros usuarios, familias y comunidad urbana y rural.

Objetivos Estratégicos

Estratégico Nro. 3: Enfoque a la Gestión y Desempeño – SOGC – Procesos y Procedimiento – Innovación – Tecnología – Sistemas De Información justificación: Esta política permite proteger los sistemas de información, los datos personales y la infraestructura tecnológica que soportan los procesos administrativos y asistenciales. Al implementar controles de ciberseguridad, gestión de accesos, respaldo de información y medidas contra incidentes digitales, se garantiza la continuidad operativa, la confianza institucional y la integridad de los servicios prestados, aspectos esenciales para un soporte institucional robusto, seguro y alineado con la transformación digital del sector salud.

Valor asociado a la Política

Responsabilidad:

Entendido como el compromiso de actuar con diligencia, rigor y conciencia institucional en el uso, protección y gestión de la información digital. La responsabilidad de cada servidor público frente a los activos tecnológicos y los datos institucionales es clave para garantizar la seguridad, la continuidad de los servicios y la confianza de la ciudadanía en los sistemas de salud. Este valor impulsa una cultura organizacional que previene incidentes, protege los derechos de los titulares de la información y asegura la trazabilidad institucional.

3. ENUNCIADO

La Subred Integrada de Servicios de Salud Sur E.S.E. se compromete a garantizar el uso adecuado y responsable de los recursos informáticos y tecnológicos de la entidad, promoviendo la protección de la información institucional y de los datos personales que se gestionan en el marco de la prestación de los servicios de salud.

Para ello, se velará por preservar en todo momento los principios de **confidencialidad, integridad y disponibilidad de la información**, mediante la identificación, gestión y mitigación de los riesgos, amenazas y posibles impactos que puedan afectar la continuidad, eficiencia y calidad de los servicios.
Este compromiso incluye la aplicación de la normatividad vigente en materia de protección de datos, seguridad digital y gobierno en línea, así como la adopción de controles, buenas prácticas y estándares internacionales que fortalezcan la confianza de los usuarios y la comunidad en la gestión de la Subred.

4. OBJETIVO DE LA POLÍTICA

Promover una cultura organizacional orientada al uso responsable y seguro de la información como insumo fundamental para la toma de decisiones basadas en hechos y datos. Para ello, se implementarán lineamientos, controles y prácticas de seguridad que aseguren la protección de los activos de información, garantizando su confidencialidad, integridad, disponibilidad y confiabilidad, independientemente de la forma en que la información sea generada, compartida, comunicada, procesada o almacenada.

5. ALCANCE DE LA POLÍTICA

La presente política es de obligatorio cumplimiento y aplica sin excepción a todos los procesos, áreas y servicios de la Subred Integrada de Servicios de Salud Sur E.S.E.

Su cumplimiento es responsabilidad de todos los colaboradores de planta, contratistas, practicantes, terceros, proveedores y aliados estratégicos, sean personas naturales o jurídicas, que tengan acceso, administren, procesen, almacenen, transmitan o gestionen información o recursos tecnológicos de la entidad, ya sea de manera directa o indirecta.

Este alcance incluye la información en cualquier formato o medio (físico, electrónico, audiovisual, magnético, nube u otros), los activos tecnológicos que la soportan, así como las interacciones con entidades públicas o privadas que presten servicios o suministren productos a la Subred.

6. DEFINICIONES

ACCESO REMOTO: Posibilidad de realizar ciertas tareas en una computadora (ordenador) sin estar físicamente en contacto con el equipo.

ACTIVO DE INFORMACIÓN: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Subred Sur ESE y, en consecuencia, debe ser protegido.

ACUERDO DE CONFIDENCIALIDAD: Es un documento en los que los colaboradores y contratistas de la

Subred Sur ESE o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Subred Sur ESE, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

ATI - ADMINISTRADORES DE TECNOLOGÍAS DE INFORMACIÓN: Responsables de la administración de los equipos de cómputo, sistemas de información y redes de la Subred Sur ESE. Velan por todo lo relacionado con la utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

AUTENTICACIÓN: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CAPACITY PLANNING: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

CENTROS DE CABLEADO: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

CENTRO DE CÓMPUTO: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

CIFRADO: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para a los repositorios de información. Prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido CRIPTOGRAFÍA: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

CUSTODIO DEL ACTIVO DE INFORMACIÓN: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

DECLARACIÓN DE APLICABILIDAD: Documento que enumera los controles aplicados por el SGS1 de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección corno de la exclusión de controles incluidos en el anexo A de la norma

DERECHOS DE AUTOR: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

DISPONIBILIDAD: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

DISPOSITIVOS LOT: consiste en un objeto al que se le ha dotado de conexión a Internet y cierta inteligencia software, sobre el que se pueden medir parámetros físicos o actuar remotamente y que por tanto permite generar un ecosistema de servicios alrededor del mismo.

EQUIPO DE CÓMPUTO: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

GUÍAS DE CLASIFICACIÓN DE LA INFORMACIÓN: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

HACKING ÉTICO: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar danos en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

IDENTIFICACIÓN DEL RIESGO: Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la Subred Sur, que ponen en riesgo la Confidencialidad, Integridad y Disponibilidad de los Activos de Información, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

INCIDENTE DE SEGURIDAD: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo). INGENIERÍA SOCIAL: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

INTEGRIDAD: Es la protección de la exactitud y estado completo de los activos.

INVENTARIO DE ACTIVOS DE INFORMACIÓN: Es una lista ordenada y documentada de los activos de información pertenecientes a la Subred Sur ESE.

LICENCIA DE SOFTWARE: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

MEDIO REMOVIBLE: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

PERFILES DE USUARIO: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

POLÍTICA DE SEGURIDAD: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

PROPIEDAD INTELECTUAL: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

PROPIETARIO DE LA INFORMACIÓN: Es la unidad organizacional o proceso donde se crean los activos de información.

RECURSOS TECNOLÓGICOS: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de La Subred Sur ESE.

REGISTROS DE AUDITORIA: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de La Subred Sur ESE. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

RESPONSABLE POR EL ACTIVO DE INFORMACIÓN: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo

SISTEMA DE INFORMACIÓN: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por La Subred Sur ESE ❑ de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SISTEMAS DE CONTROL AMBIENTAL: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

SOFTWARE MALICIOSO: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

TERCEROS: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

TRABAJO EN CASA: Trabajo que se realiza en un lugar alejado de las oficinas centrales, de las instalaciones de producción o del cliente que lo contrata, mediante la utilización de las nuevas tecnologías de la información y la comunicación.

USUARIO: En el presente documento se emplea para referirse a directivos, colaboradores, contratistas, terceros y otros colaboradores de la Subred Sur ESE, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Subred Sur ESE y a quienes se les otorga un nombre de usuario y una clave de acceso.

VULNERABILIDADES: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Subred Sur ESE (amenazas), las cuales se constituyen en fuentes de riesgo.

7. DESARROLLO

La Subred Integrada de Servicios de Salud Sur E.S.E., entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita establecer un marco de confianza en el cumplimiento de sus deberes con el Estado, los ciudadanos, los pacientes y demás grupos de valor, en estricto cumplimiento de la normatividad vigente y en coherencia con su misión y visión institucional.

La protección de la información busca reducir los riesgos e impactos asociados a las amenazas que puedan afectar los activos de información de la entidad. Los riesgos serán identificados y gestionados de manera sistemática con el fin de mantener un nivel de exposición aceptable que garantice la confidencialidad, integridad, disponibilidad y confiabilidad de la información, de acuerdo con las necesidades de los diferentes grupos de interés.

En concordancia con lo definido en el alcance, el desarrollo de las acciones y la toma de decisiones en materia de seguridad de la información estarán basados en principios de legalidad, responsabilidad, proporcionalidad, transparencia, necesidad y seguridad.
La Subred se compromete a:

- **Fortalecer la cultura de seguridad de la información** en todos los colaboradores, proveedores, contratistas, consultores y terceros vinculados, garantizando la continuidad del negocio frente a incidentes de seguridad.
- **Definir, implementar, operar y mejorar continuamente el SGSI**, alineado con las necesidades institucionales, los riesgos identificados y los requerimientos regulatorios y contractuales.
- **Promover la sensibilización y formación permanente** en seguridad de la información, de manera que cada actor conozca y asuma sus responsabilidades en la protección de los activos de información.

Principios rectores de seguridad de la información

La Subred establece los siguientes principios que sustentan su SGSI:

1. Las responsabilidades frente a la seguridad de la información serán claramente definidas, publicadas, socializadas y aceptadas por cada colaborador, contratista, proveedor o consultor vinculado con la entidad.
2. La información generada, procesada o resguardada por los procesos de negocio será protegida frente a los riesgos derivados del acceso de terceros (proveedores, clientes, outsourcing) o de usuarios internos.
3. La información creada, procesada, transmitida o almacenada por la Subred será protegida para minimizar impactos financieros, legales, operativos o reputacionales, aplicando controles de acuerdo con su clasificación y criticidad.
4. La Subred protegerá la información contra amenazas originadas por el personal, mediante la adopción de medidas de control interno y campañas de concientización.
5. Las instalaciones y la infraestructura tecnológica que soportan los procesos críticos serán protegidas frente a accesos no autorizados, desastres o incidentes de seguridad.
6. Los procesos de negocio serán controlados de manera que se garantice la seguridad de los recursos tecnológicos, las aplicaciones y las redes de datos.
7. El acceso a la información, sistemas y recursos de red será gestionado mediante controles de autenticación, autorización y trazabilidad.
8. La seguridad de la información será considerada desde la planeación, diseño, desarrollo, implementación y operación de cada sistema o solución tecnológica.
9. Los eventos e incidentes de seguridad, así como las debilidades identificadas en los sistemas de información, serán gestionados de forma oportuna para fortalecer de manera continua el modelo de seguridad.
10. Se garantizará la disponibilidad de los procesos de negocio y la continuidad operativa mediante planes de contingencia, recuperación y continuidad del negocio.

11. Se velará por el cumplimiento estricto de las obligaciones legales, regulatorias, contractuales y de auditoría, nacionales e internacionales, relacionadas con la seguridad de la información.
12. Se fomentará la mejora continua del Sistema de Gestión de Seguridad de la Información, incorporando las lecciones aprendidas de incidentes, auditorías y revisiones periódicas.

8. NIVELES DE RESPONSABILIDAD SOBRE EL SEGUIMIENTO Y EVALUACIÓN

En el marco del Modelo Integrado de Planeación y Gestión (MIPG), la Subred Integrada de Servicios de Salud Sur E.S.E. establece los siguientes niveles de responsabilidad para la gestión, seguimiento y evaluación de la Política de Seguridad de la Información:

- **Línea Estratégica**: a cargo de la Gerencia, responsable de definir el marco general de la política, establecer las directrices institucionales y supervisar su cumplimiento, garantizando la alineación con la misión, visión y objetivos estratégicos de la entidad.

- **Primera línea de defensa**: a cargo de la **Jefatura de Sistemas de Información y TIC**, cuya responsabilidad es divulgar y socializar la política, liderar su implementación en los procesos de la entidad, realizar seguimiento a las acciones definidas en el autocontrol, así como coordinar y diligenciar la autoevaluación en el marco del MIPG.
- **Segunda línea de defensa**: a cargo de la **Oficina Asesora de Desarrollo Institucional**, encargada de monitorear la implementación de la política, medir y analizar los indicadores asociados, evaluar la eficacia de las estrategias definidas y verificar la gestión desarrollada por la primera línea de defensa.

- **Tercera línea de defensa**: a cargo de la **Oficina de Control Interno**, responsable de proveer una evaluación independiente, objetiva y de aseguramiento mediante auditorías internas que valoren la efectividad de la política, la pertinencia de su implementación y la adecuada operación del Sistema de Control Interno.

9. INDICADORES

OBJETIVO QUE SE DESEA ALCANZAR CON EL CUMPLIMIENTO DE LA POLÍTICA	METAS PARA DAR CUMPLIMIENTO AL OBJETIVO ESPECÍFICO DE LA POLÍTICA	INDICADOR DE EVALUACIÓN		
		NOMBRE DEL INDICADOR	FÓRMULA	PERIODICIDAD DE MEDICIÓN
Realizar seguimiento, monitoreo y evaluación a las actividades definidas en el Plan *de* Seguridad de la información.	Cumplir mayor o igual 90% de las actividades definidas en el plan Seguridad de la Información.	Porcentaje de cumplimiento del Plan de Seguridad de la Información	Número de actividades ejecutadas de acuerdo al cronograma definido / Total de actividades programadas *100	Trimestral

10. PUNTO DE CONTROL

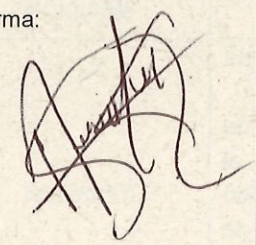
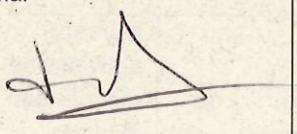
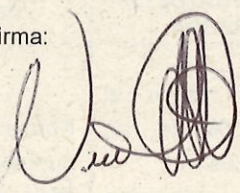
Seguimiento de los indicadores de acuerdo a su periodicidad a través de la mesa Acreditación Gerencia de la Información Comité Seguridad de la Información.

11. RESPONSABLE

Jefe de Oficina Sistemas de Información TICS.

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	05/11/2019	Articulación con los lineamientos de MIPG.
2	27/07/2021	Articulación con la Plataforma estratégica 2020-2024, Inclusión de los controles definidos por el Ministerio de las Tics. Definición de los indicadores que soportan el plan de Seguridad de la Información.
3	04/10/2023	Actualización de la normativa y enfoque del objetivo de la política de seguridad.
4	18/08/2026	Actualización de normatividad y articulación con la Plataforma Estratégica 2024-2028.

ELABORADO POR	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Andrés Felipe Cubillos García.	Nombre: Julio Andrés Sánchez Sánchez.	Nombre: Nicolas Suarez Casallas.	Nombre: Viviana Marcela Clavijo.
Cargo: Profesional especializado Seguridad informática e Información.	Cargo: Jefe Oficina Sistemas de Información TICS.	Cargo: Jefe Oficina Asesora de Desarrollo Institucional.	Cargo: Gerente.
Fecha: 18/08/2026	Fecha: 18/08/2026	Fecha: 20/08/2026	Fecha: 20/08/2026
Firma: 	Firma: 	Firma: 	Firma: