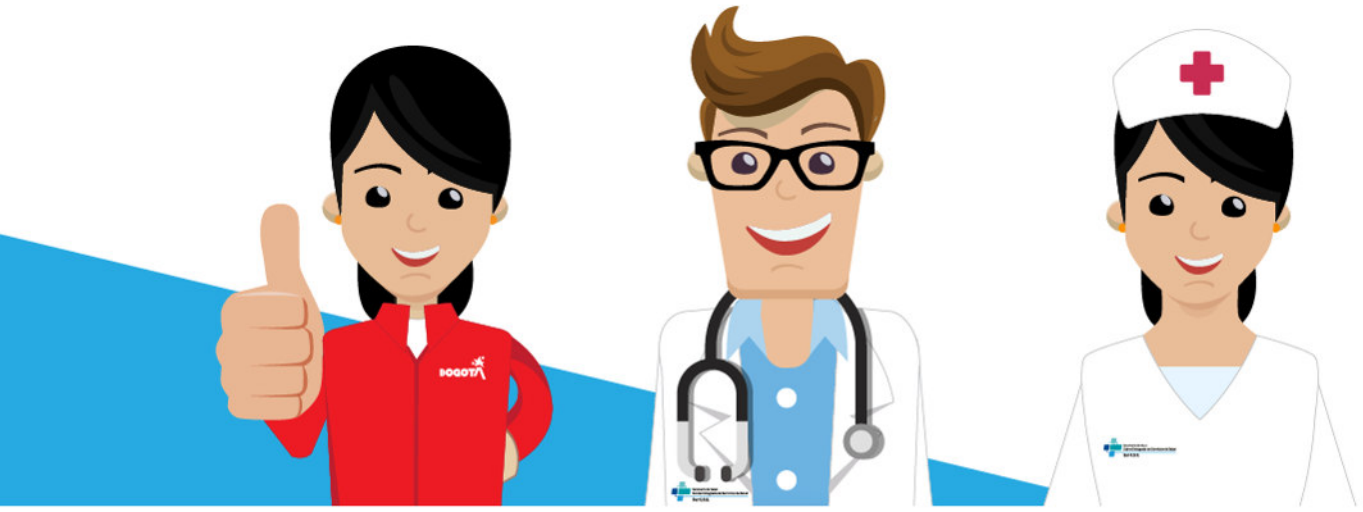
SUBRED INTEGRADA DE SERVICIOS DE SALUD SUR E.S.E

PLAN

TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GI-TIC-PL-05 V7



Secretaría de Salud
Subred Integrada de Servicios de Salud
Sur E.S.E.

BOGOTÁ

1. INTRODUCCIÓN:

El objetivo primordial del Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, es garantizar que éstos sean conocidos, gestionados y tratados por la Entidad de una forma documentada, sistemática, estructurada, repetible y eficiente, para lo cual es esencial identificar y valorar los riesgos que pueden afectar la seguridad y privacidad de la información, y por consiguiente establecer los mecanismos más convenientes para protegerla.

Lo anterior implica, que la Entidad requiere conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, y conocer los posibles riesgos que puedan afectar la seguridad y privacidad de los mismos y de esta forma determinar las medidas orientadas a minimizar el impacto en caso de presentarse la materialización de una amenaza.

En la medida que se tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, la Entidad puede establecer controles y medidas efectivas, viables y transversales, con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de su información, para lo cual es necesario definir los lineamientos que se deben seguir, para el análisis y evaluación de los riesgos de Seguridad de la Información de la Entidad.

2. OBJETIVO:

- Actualizar e implementar directrices internas que orienten a la institución en la correcta identificación, análisis, valoración y seguimiento de los riesgos de seguridad y privacidad de la información, los cuales puedan afectar el logro de los objetivos institucionales o la atención centrada en el usuario. Estas directrices se desarrollarán en el marco de los procesos, proyectos y/o planes, con el fin de minimizar la ocurrencia de dichos riesgos mediante acciones de control efectivas.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Mantener la integridad, confidencialidad y disponibilidad de la información a través de la gestión del riesgo asociado a la información de la Subred Integrada de Servicios de Salud Sur E.S.E.

3. ALCANCE:

Los lineamientos presentados en este documento son aplicables a todos los procesos de la Subred Integrada de Servicios de Salud Sur E.S.E., con alcance a los colaboradores de todos los niveles del orden asistencial o administrativos.

DESDE: La identificación de los Riesgos de Seguridad y privacidad de la información.

HASTA: El seguimiento y mejora de la gestión de riesgos de Seguridad y privacidad de la información.

4. DEFINICIONES:

ACTIVO DE INFORMACIÓN: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

AMENAZA: Es la causa potencial de un daño a un activo de información.

ANÁLISIS DE RIESGOS: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

CAUSA: Razón por la cual el riesgo sucede.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible a personas no autorizados

CONTROLES: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

DISPONIBILIDAD: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

IMPACTO: Consecuencias de que la amenaza ocurra.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

PROBABILIDAD DE OCURRENCIA: Posibilidad de que se presente una situación o evento específico.

RIESGO: Grado de exposición de un activo que permite la materialización de una amenaza.

RIESGO INHERENTE: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

RIESGO RESIDUAL: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: permite establecer,

implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

VULNERABILIDAD: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

5. NORMATIVIDAD APLICABLE:

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Ley 1582	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Congreso de Colombia
Ley 1928	2019	Normativa sobre el uso y almacenamiento seguro de información biométrica en Colombia.	Congreso de Colombia
Ley de Protección de Datos de Salud (HIPAA - Estados Unidos)	2021	Reglamento para la seguridad y privacidad en el manejo de información de salud en EE.UU., relevante para organizaciones con datos de pacientes internacionales.	Departamento de Salud y Servicios Humanos de EE.UU.

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Ley 2300	2023	Nueva normativa colombiana que regula el uso responsable de datos personales y amplía la Ley 1581 de 2012.	Congreso de Colombia
Decreto 1377	2013	Reglamenta parcialmente la Ley 1581 de 2012 y establece las condiciones y procedimientos para garantizar el adecuado manejo de la información personal. En el contexto de un Plan de Tratamiento de Riesgos, este decreto es crucial para entender las obligaciones relacionadas con la privacidad de la información.	Presidencia
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	MINTIC
Decreto 767	2022	Regulación que actualiza el marco normativo de seguridad digital en Colombia, alineado con estándares internacionales.	Presidencia de la República de Colombia
Resolución 1995	1999	Define las normas técnicas y administrativas para la protección de la confidencialidad de la información en el sector salud. Aunque inicialmente se centra en el ámbito de la salud, sus principios y lineamientos son útiles para otras entidades que manejan información sensible.	Ministerio de Salud
NTC/ISO 31000	2009	Gestión del Riesgo. Principios y directrices	ICONTEC
NTC / ISO 27001	2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).	ICONTEC
ISO/IEC 27001	2013	brinda un marco de referencia para el establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Muchas organizaciones adoptan esta norma para fortalecer sus prácticas de seguridad de la información.	ICONTEC
ISO/IEC 27017	2015	Controles específicos para la seguridad en entornos de computación en la nube, aplicables a proveedores y clientes.	ISO
ISO/IEC 27035	2016	Estándar para la gestión de incidentes de seguridad de la información, estableciendo procesos para la detección, respuesta y aprendizaje de incidentes.	ISO
NIST SP 800-30	2016	Guía de Gestión de Riesgos para los Sistemas de Tecnología de la Información	NIST

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Modelo de Gestión de Riesgos de Seguridad Digital	2017	Modelo de Gestión de Riesgos de Seguridad Digital	MINTIC
Reglamento General de Protección de Datos (GDPR - Europa)	2018	Marco regulador para la protección de datos personales en la Unión Europea, aplicable a organizaciones internacionales.	Parlamento Europeo y Consejo de la UE
ISO/IEC 27018	2019	Estándar para la protección de datos personales en entornos de computación en la nube, asegurando la privacidad de los datos almacenados.	ISO
ISO/IEC 27701	2019	Extensión de la norma ISO/IEC 27001 para la gestión de la privacidad de la información y cumplimiento con regulaciones como la GDPR.	ISO
NIST 800-207 (Zero Trust Security)	2020	Modelo de seguridad basado en la verificación continua y restricciones de acceso, minimizando los riesgos de brechas de seguridad.	NIST
ISO/IEC 27001	2022	Versión actualizada del estándar de gestión de seguridad de la información, con nuevos controles para ciberseguridad, resiliencia y seguridad en la nube.	Organización Internacional de Normalización (ISO)
ISO/IEC 27002	2022	Controles actualizados para la gestión de seguridad de la información, alineados con ISO 27001:2022.	ISO
ISO/IEC 27001	2022	Versión actualizada del estándar de gestión de seguridad de la información, con nuevos controles para ciberseguridad, resiliencia y seguridad en la nube.	Organización Internacional de Normalización (ISO)
ISO/IEC 27002	2022	Controles actualizados para la gestión de seguridad de la información, alineados con ISO 27001:2022.	ISO
ISO/IEC 23894	2023	Directrices para la gestión de riesgos en sistemas de Inteligencia Artificial, asegurando el uso responsable de la IA en la seguridad de la información.	ISO
NIST Cybersecurity Framework (CSF)	2023	Nueva versión del marco de ciberseguridad del NIST, con enfoque en Zero Trust y protección de infraestructuras críticas.	NIST

6. RESPONSABLES:

El responsable de la elaboración y actualización del presente Plan es la Oficina de Sistemas de Información TICS, quien a su vez se encargará de la evaluación y adherencia del mismo, de manera anual.

7. CONTENIDO DEL PLAN:

7.1. ARTICULACION CONTEXTO ESTRATEGICO INSTITUCIONAL

MISIÓN: La Subred Integrada de Servicios de Salud Sur ESE, presta Servicios de Salud a través de un Modelo de Atención Integral en Red, bajo los enfoques de Gestión Integral del Riesgo, Seguridad, fortaleciendo la formación académica orientada a la investigación Científica e innovación, con un Talento Humano Comprometido, Humanizado y Competente que contribuya al mejoramiento de las condiciones de salud de nuestros usuarios urbanos y rurales de las localidades de Usme, Ciudad Bolívar, Tunjuelito y Sumapaz.

VISIÓN: En el 2024 seremos una Empresa Social del Estado referente en el Distrito por la Prestación de Servicios de Salud con Estándares Superiores de Calidad, Consolidada, Sostenible, referente en investigación, Docencia e Innovación, con Enfoque Diferencial, Territorial y comunitario, que promueven el cambio, la intersectorial ida, impactando positivamente la salud y calidad de vida de nuestros usuarios.

VALORES INSTITUCIONALES: Los valores son aptitudes o cualidades individuales que definen la conducta de un individuo de la sociedad. Dichos valores derivan de los principios éticos universales, de allí que su objetivo sea guiar a los individuos a obrar correctamente, de forma individual y colectiva.

Tomando como referencia lo establecido en el Decreto Distrital 118 de 2018, Política de Integridad de la Dimensión de Talento Humano, que adopto cada una de las Entidades Públicas del Distrito Capital.

No.	VALOR	DEFINICIÓN
1	Honestidad	Es un valor moral fundamental para entablar relaciones interpersonales basadas en la confianza, la sinceridad y el respeto mutuo.
2	Respeto	Es un sentimiento positivo, que se refiere a la acción de respetar; es equivalente a tener veneración, aprecio y reconocimiento por una persona o cosa.
3	Compromiso	Es una obligación contraída, palabra dada.
4	Justicia	Es un conjunto de valores esenciales sobre los cuales debe basarse una sociedad y el Estado, Estos valores son el respeto, la equidad, la igualdad y la libertad.
5	Diligencia	Es el cuidado y el esmero en ejecutar o realizar algo. Es esa prontitud de ánimo, esa agilidad interior y exterior, esa prisa pacifica en hacer bien, en hacer con amor, en hacer con alegría lo que tengo me corresponden en ese momento.

PRINCIPIOS INSTITUCIONALES

Los principios son reglas o normas que orientan la acción de un ser humano cambiando las facultades espirituales racionales. Se trata de normas de carácter general y universal, como, por ejemplo: amar al prójimo, no mentir, respetar la vida de las demás personas, etc. Los principios morales también se llaman máximas o preceptos constitucionales.

Tomando como referencia lo establecido en el artículo 5 del Acuerdo Distrital 761 de 2015, por el cual se adopta el Plan de Desarrollo Económico, Social, Ambiental y de Obras Públicas para Bogotá 2020-2024: "Un Nuevo contrato Social y Ambiental Para la Bogotá del Siglo XXI".

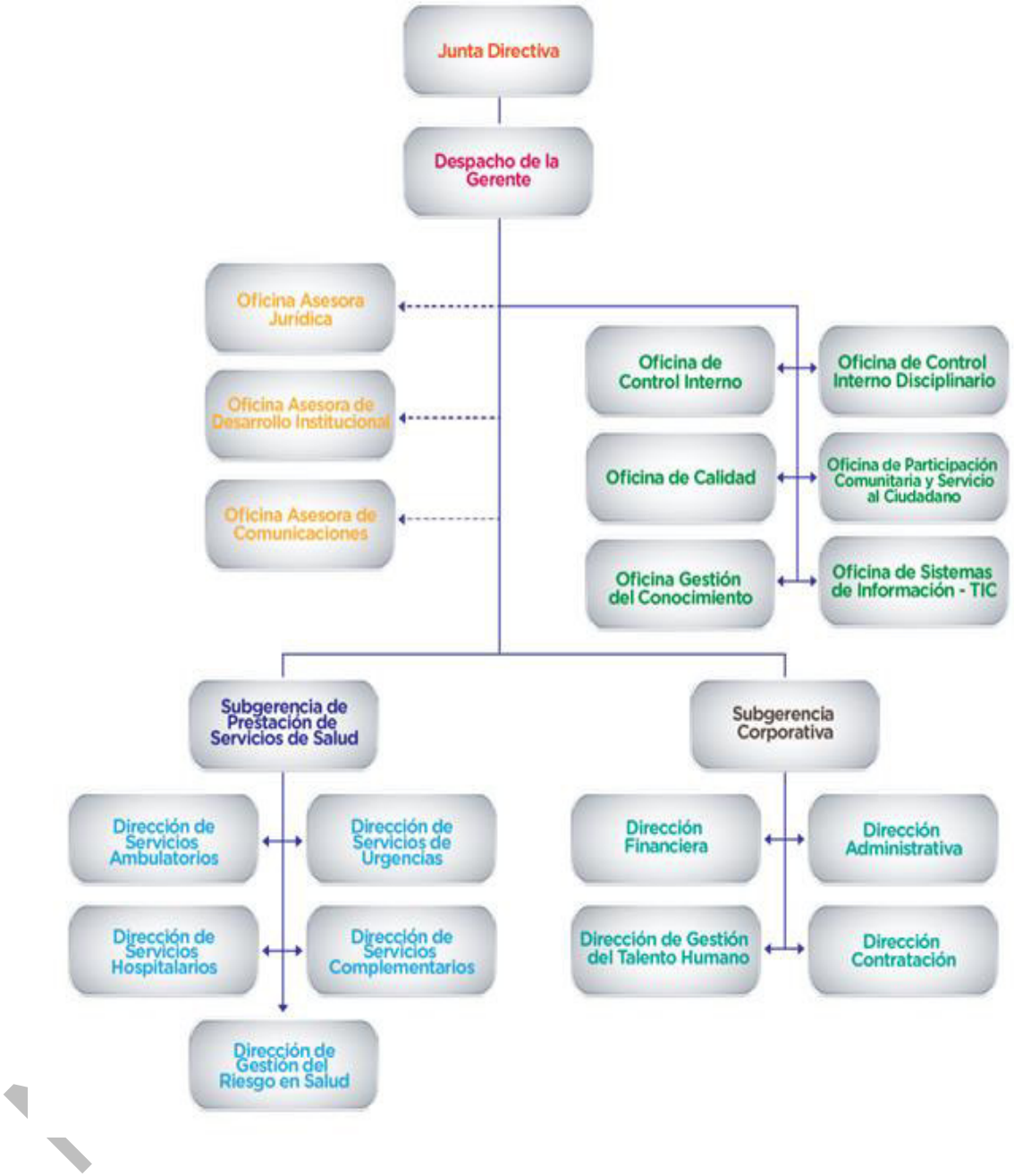
1. Vocación de Servicio y Liderazgo Público.
2. Ética.
3. Transparencia y Rendición de Cuentas.
4. Inteligencia y Acción Colectiva.
5. Corresponsabilidad.
6. Interdependencia e Integración.

OBJETIVOS ESTRATÉGICOS

En la definición de los objetivos estratégicos, se contempla a continuación los adelantos de los propósitos entregados por los líderes de los procesos y sus equipos de Trabajo, las líneas técnicas de la propuesta del Plan Territorial en Salud y lo dispuesto por las líneas de Secretaria Distrital de Salud, a continuación, se presenta los avances:

1. Consolidar el Modelo de Atención Integral en Red, garantizando la Prestación de Servicios Integrales de Salud, con enfoque en la Gestión de Riesgos, Servicios Humanizados, Accesibles y Oportunos, impactando positivamente las condiciones de Salud de nuestros Usuarios, Familias y Comunidades.
2. Alcanzar estándares superiores de calidad en salud, mediante la implementación de acciones progresivas que contribuyan al fortalecimiento del desempeño institucional y reconocimiento como Hospital Universitario de la Subred Sur ESE. Optimizando la atención centrada en los usuarios.
3. Administrar adecuadamente, eficaz, eficiente y transparente los Recursos Financieros que conlleven a una sostenibilidad financiera de la Subred Sur que contribuya en la Prestación Integral de Servicios.
4. Fortalecer la Cultura Organizada y el Crecimiento del Talento Humano a través del desarrollo de competencias laborales, que promuevan una cultura de servicio humanizado y de mejoramiento continúo facilitando la implementación del Modelo de Atención en Red.
5. Mantener los niveles de satisfacción de los Usuarios, Familia y Comunidad, desarrollo estrategias que promuevan los espacios de participación y fortalecimiento del control social a partir del modelo de atención en red.

ESTRUCTURA ORGANIZACIONAL:



MAPA DE PROCESOS

El proceso de gestión de la información TIC depende de la Oficina de Sistemas de información TIC, y se consolida como un proceso estratégico en el mapa de procesos de la entidad.

7.2. ARTICULACION CON LA POLÍTICA DE GESTION DE RIESGOS

La Subred Integrada de Servicios de Salud Sur E.S.E. por medio de la presente política se compromete con la gestión y control integral de los riesgos identificados en los procesos, mediante un ejercicio integral y articulado entre el componente asistencial y administrativo, para continuar prestando servicios de salud integrales y resultados de desempeño institucional, acorde con el Modelo de Atención vigente y la Política de Atención integral en salud.

OBJETIVO: Establecer los lineamientos "unificados" para la administración de las tipologías de riesgo definidas en la institución, mediante un enfoque integral que permita fortalecer la cultura de prevención y control de riesgos con participación activa de los colaboradores y operación de líneas de defensa, para contribuir al logro de los objetivos estratégicos y continuidad en la Prestación de servicios de salud acorde con el modelo de atención en Salud y Política de Atención integral en salud.

7.3. ARTICULACION CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Subred Integrada de Servicios de Salud Sur E.S.E. por medio de la presente política se compromete a mantener la confidencialidad, integridad y disponibilidad de la información a través de la identificación y mitigación de los riesgos a los cuales está expuesta con el objeto de asegurar la misma y propender por el establecimiento de una cultura de seguridad informática.

OBJETIVO: Mantener la seguridad informática de la Subred Integrada de Servicios de Salud Sur E.S.E. con el fin de disponer de información confiable, integra y oportuna que facilite la toma de decisiones institucionales.

7.4. ARTICULACION CON MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN MIPG

El Gobierno Nacional ha diseñado sistemas y modelos para orientar a las entidades públicas en el ejercicio de la gestión institucional y el control interno, con el fin de fortalecer el desempeño y la generación de valor público. El Modelo Integrado de Planeación y Gestión (MIPG) articula los Sistemas de Gestión y de Control Interno, armoniza los procesos institucionales y brinda un panorama integral para la toma de decisiones.

En este marco, la Subred Integrada de Servicios de Salud Sur E.S.E. adopta como referencia metodológica para la administración del riesgo y el diseño y valoración de controles la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 del Departamento Administrativo de la Función Pública (DAFP), en concordancia con su Manual de Administración del Riesgo DI-GRI-MA-01 y con la Política Institucional de Gestión del Riesgo.

Para los riesgos de Seguridad y Privacidad de la Información, la metodología se complementa con los lineamientos del MSPI y con buenas prácticas de ISO/IEC 27001, considerando los riesgos inherentes asociados a la confidencialidad, integridad y disponibilidad de los activos de información.

En la valoración se aplican criterios de probabilidad (asociada a la frecuencia) e impacto (incluyendo afectación económica y reputacional), para determinar la zona de riesgo y orientar controles y acciones de tratamiento proporcionales y verificables.

Una de las políticas vinculadas al Modelo es la Política de Gestión de la Información y las Comunicaciones (TIC), la cual opera en la Dimensión 3 "Gestión con valores para resultados", bajo los siguientes atributos:

1. La gestión de la entidad se soporta en:
    - El trabajo por procesos, el cual tiene en cuenta los requisitos legales, las necesidades de los grupos de valor, las políticas internas de la entidad y los cambios del entorno, para brindar resultados con valor.
    - El uso de las TIC para tener una comunicación fluida con la ciudadanía y atendiendo las políticas de Gobierno Digital y Seguridad.
    - La consulta de las disposiciones legales que regulan su gestión

- Una estructura organizacional articulada con los procesos y que facilita su interacción, en función de los resultados institucionales
- El compromiso con la preservación del medio ambiente
- Trámites simples y eficientes que faciliten el acceso de los ciudadanos a sus derechos
- La promoción de espacios de participación ciudadana que evalúa para generar acciones de mejora

2. La delegación o tercerización (cuando procede) de procesos, bienes y/o servicios se ajusta a los requerimientos de la entidad y a sus grupos de valor.
3. El uso de los recursos disponibles atiende las políticas de transparencia, integridad y racionalización del gasto público.
4. Los procesos judiciales en los que intervenga la entidad cumplen parámetros de pertinencia y oportunidad dentro del ámbito de la legalidad.
5. La entidad rinde permanentemente cuentas de su gestión promoviendo la transparencia, la participación y la colaboración de los grupos de valor y grupos de interés.
6. La entidad establece mecanismos de fácil acceso y comprensibles para que los grupos de valor presenten sus PQRSD.
7. La entidad responde de manera clara, pertinente y oportuna, las PQRSD y son insumo para la mejora continua en sus procesos.

Con base en la metodología adoptada (DAFP - Versión 6), la administración de los riesgos de Seguridad y Privacidad de la Información de la Subred Integrada de Servicios de Salud Sur E.S.E. se orienta a promover una cultura de riesgos con enfoque en resultados y en la mitigación de eventos que puedan afectar la gestión institucional o la prestación del servicio, a través de la aplicación de cuatro (4) fases.

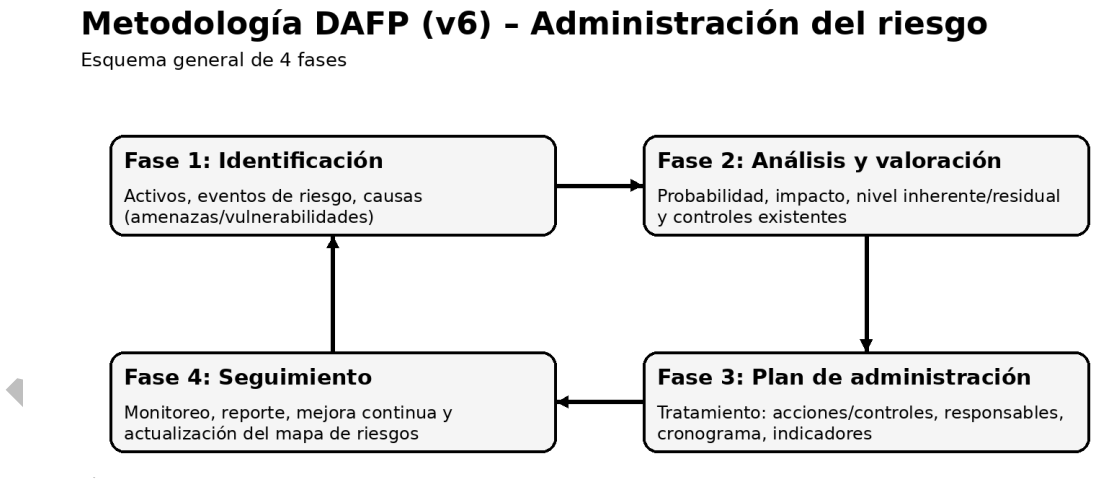


Figura 3. Metodología DAFP (v6) para la administración del riesgo – Esquema general de 4 fases.

7.4.1.Fase 1. Identificación:

En esta fase se identifican los riesgos de Seguridad y Privacidad de la Información, a partir del inventario de activos, los procesos asociados y el contexto de la Subred.

- Inventariar/actualizar activos de información y responsables (dueños del activo).
- Identificar eventos de riesgo sobre confidencialidad, integridad y disponibilidad.
- Determinar causas (amenazas y vulnerabilidades) y consecuencias potenciales.
- Documentar el riesgo en el mapa institucional (riesgo, activo, tipo, causa y consecuencia).

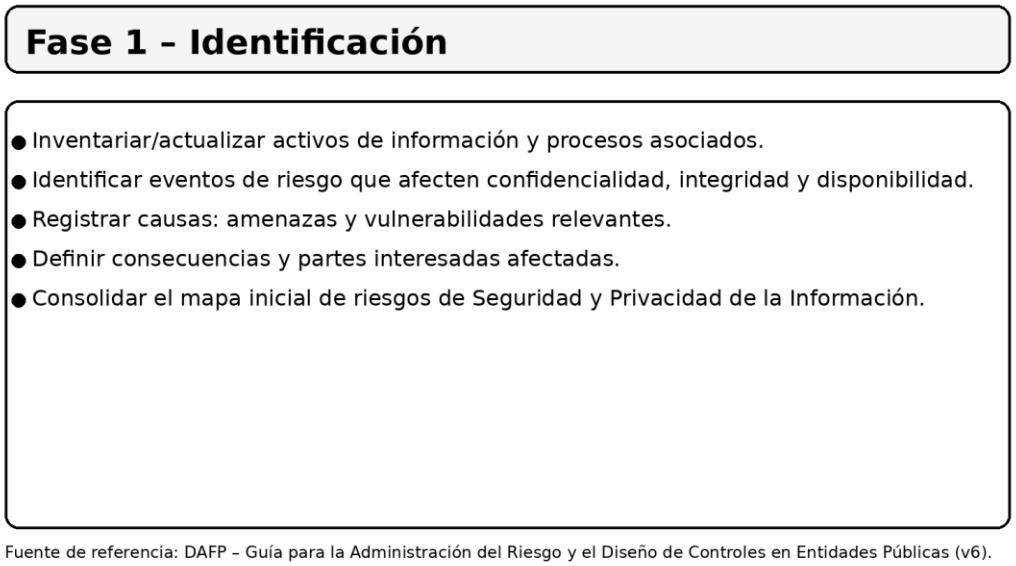


Figura 4. Fase 1 – Identificación (resumen operativo).

7.4.2. Fase 2. Análisis y valoración:

Una vez identificados, los riesgos se analizan y valoran para estimar su nivel, priorizar su tratamiento y determinar el riesgo residual considerando los controles existentes.

- Estimar probabilidad e impacto con criterios institucionales (metodología DAFP/MIPG).
- Valorar el diseño y la efectividad de los controles existentes.
- Determinar el nivel de riesgo inherente y residual, y ubicarlo en la matriz.
- Priorizar riesgos de acuerdo con su nivel y con el apetito/tolerancia al riesgo.

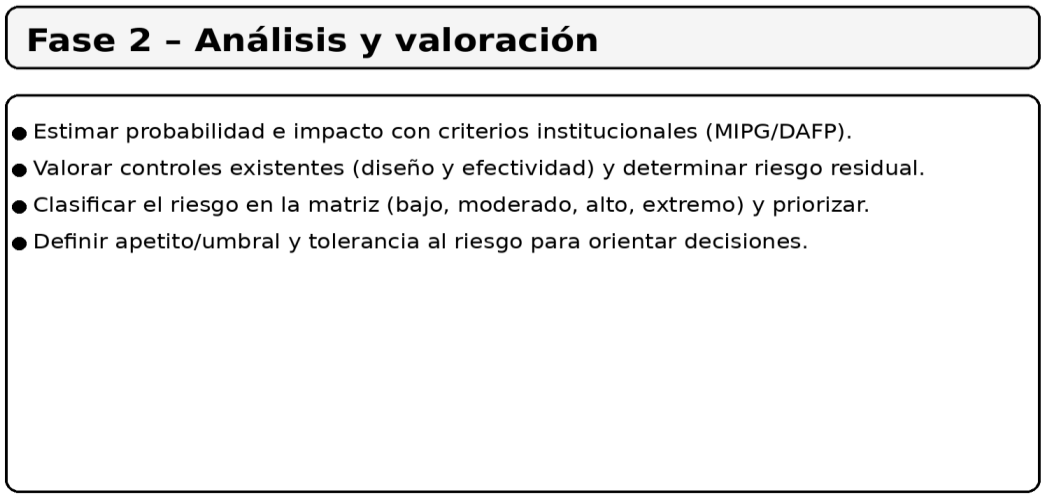


Figura 5. Fase 2 – Análisis y valoración (resumen operativo).

7.4.3. Fase 3. Diseño plan de administración del riesgo:

En esta fase se define el plan de administración del riesgo (tratamiento), estableciendo acciones y controles orientados a la causa del riesgo, con responsables, tiempos e indicadores.

- Seleccionar opción de tratamiento: reducir/mitigar, evitar, compartir o aceptar.
- Definir controles y acciones (preventivos, detectivos y correctivos) y su soporte documental.
- Asignar responsables, recursos y cronograma; definir evidencias de implementación.
- Establecer indicadores de eficacia/efectividad y metas para el seguimiento.

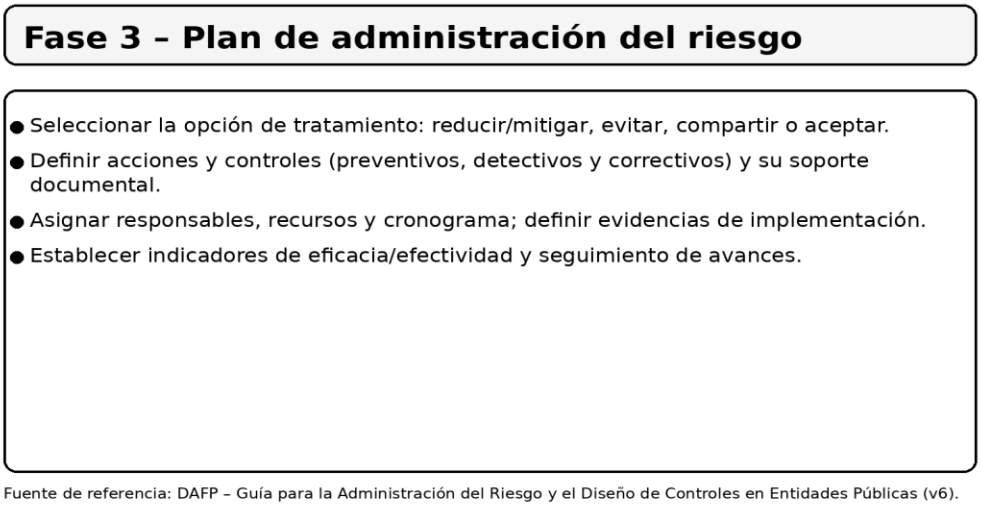


Figura 6. Fase 3 – Plan de administración del riesgo (resumen operativo).

7.4.4. Fase 4. seguimiento de los riesgos:

En esta fase se realiza seguimiento desde las tres líneas de defensa:

i. La de primer Orden el jefe de Oficina de sistemas de información TICS durante la aplicación de las acciones de seguimiento manteniendo trazabilidad y/o documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable, que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplirán.

ii. En el seguimiento de segundo orden la Oficina Asesora de Desarrollo Institucional. - Gerencia del Riesgo, revisa las evidencias de cumplimiento reportadas por el primer orden y valida los resultados de los indicadores.

iii. En el tercer orden, la Oficina de Control Interno como evaluador independiente de la administración del riesgo, realizará el seguimiento a los indicadores establecidos revisando el resultado general del riesgo, según verificación integral realizada por Control Interno y se describe las recomendaciones a lugar.

- Monitorear la ejecución del plan, registrar avances y recolectar evidencias.
- Revisar indicadores y resultados; actualizar el mapa de riesgos ante cambios o incidentes.
- Reportar resultados y acciones de mejora a las instancias de dirección correspondientes.

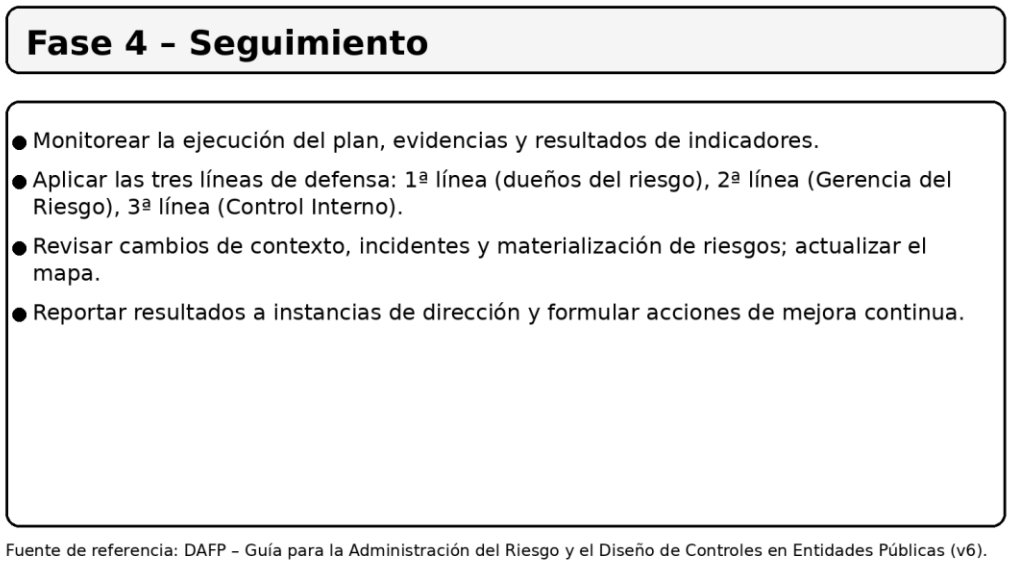


Figura 7. Fase 4 – Seguimiento (resumen operativo).

7.5. SEGUIMIENTO Y CONTROL

Para el seguimiento y control de los planes de trabajo se realizará un informe de cumplimiento por cada una de las vigencias de los cronogramas planteados para cada uno de los planes y el análisis de las fichas de los indicadores propuestos.

8. BIBLIOGRAFÍA:

1. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 (noviembre 2020)
2. EL CONGRESO DE LA REPÚBLICA, ley 1582 (30 de octubre 2012)
3. ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI) (2013)
4. https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf
5. http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf
6. http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html
7. DI-GRI-MA-01 MANUAL ADMINISTRACION DEL RIESGO, Subred Integrada de Servicios de Salud Sur E.S.E.

9. ANEXOS (Opcional):

- ANEXO 1. PLAN DE TRABAJO INSTITUCIONAL- RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2026

10. CONTROL DE CAMBIOS:

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2017-08-08	1	Creación del documento para la Subred integrada de Servicios de Salud Sur E.S. E
2021-01-21	2	Inclusión de objetivos, diagramas, inclusión de Recursos y actividades para 2021
2022-01-28	3	Cambio de código (Anterior: GI-TICS-PP-06). Inclusión de normatividad, objetivo, política de Seguridad Digital.
2023-01-30	4	Cambia de plantilla del Plan (Código anterior: MI-SIG-CDO-FT-07 V1), de acuerdo a los requerimientos normativos y se realiza actualización al documento.
2024-01-31	5	Se actualiza de acuerdo a los requerimientos normativos y se realiza actualización al documento.
2025-01-31	6	Se actualiza Normatividad y objetivos del plan.
2026-01-21	7	Actualización de articulación con modelo integrado de planeación y gestión MIPG

De conformidad con lo establecido en la Resolución 0295 de 13 de marzo de 2019, en sesión del Comité de Institucional Gestión y Desempeño de la Subred Integrada de Servicios de Salud Sur E.S.E. realizado el **28 de enero de 2026** se aprobó el presente Plan.

ELABORADO / MODIFICADO	REVISADO	CONVALIDADO	APROBADO
Nombre: Andrés Felipe Cubillos García	**Nombre:** Julio Andrés Sánchez Sánchez	**Nombre:** Sandra Patricia Alba Calderón	**Nombre:** Viviana Marcela Clavijo / Julio Andrés Sánchez Sánchez
Cargo: Profesional Especializado Seguridad Informática	**Cargo:** Jefe Oficina Sistemas Información - TIC	**Cargo**: Referente Control Documental – Oficina de Calidad	**Cargo**: Gerente / Jefe Oficina Sistemas de Información – TIC
Fecha: 2026-01-21	**Fecha:** 2026-01-27	**Fecha:** 2026-01-30	**Fecha**: 2025-01-30