

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 1 de 43 FECHA: 31/12/2022



PLAN DE TRATAMIENTO DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E.**

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 2 de 43 FECHA: 31/12/2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	4
2. JUSTIFICACIÓN	4
3. ALCANCE.....	4
4. OBJETIVO	5
5. MARCO NORMATIVO.....	5
5.1 DE ORDEN NACIONAL	5
5.2 DE ORDEN INTERNACIONAL	7
6. VOCABULARIO.....	8
7. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.....	11
7.1 FASE DE PLANIFICACIÓN	12
7.1.1 Identificación del Contexto	12
7.1.2 Modelo Operativo de Procesos	23
7.1.3 Estructura orgánica.....	31
7.1.4 Política de Gestión de Administración de Riesgos de la Subred Integrada de Servicios de Salud Norte E.S.E.....	32
7.1.5 Roles y responsabilidades.....	33
7.1.6 Identificación de Activos de información	34
7.1.7 Identificar los Riesgos.....	37
7.1.8 Valorar los riesgos	38
7.1.9 Identificación y evaluación de los controles existentes	39
7.1.10 Definición y aprobación de mapas de riesgos y planes de tratamiento	40
7.1.11 Evaluación del Riesgo residual	40
7.1.12 Plan de tratamiento de riesgos materializados.....	40
7.2 FASE DE EJECUCIÓN.....	40
7.3 FASE DE MONITOREO Y REVISIÓN.....	40
7.4 MEJORAMIENTO CONTINUO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION	41
7.5 PLAN DE TRABAJO	41
8. BIBLIOGRAFÍA.....	43

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 3 de 43
		FECHA: 31/12/2022

TABLA DE ILUSTRACIONES

<i>Ilustración 1:Proceso de gestión del riesgo en la seguridad de la información</i>	11
Ilustración 2:Modelo de Privacidad y Seguridad de la Información Vrs Proceso de Gestión de Riesgos ...	12
Ilustración 3: Alineación Estratégica	13
Ilustración 4:Mapa de procesos institucional	23
Ilustración 5: Estructura orgánica institucional	32
Ilustración 6: Rol del Oficial de Seguridad	34
Ilustración 7: Pasos para identificar y Valorar los activos de información	34
Ilustración 8: Tipología de Activos	35
Ilustración 9: Criterios Infraestructuras Críticas Cibernéticas –	37
Ilustración 10:Estructura propuesta para la redacción del riesgo	37
Ilustración 11: Criterios para definir el nivel de probabilidad.....	38
Ilustración 12: Criterios para definir el nivel de impacto.....	39
Ilustración 13:Matriz de calor	39

TABLA DE TABLAS

Tabla 1: Alineación Estratégica.....	13
Tabla 2: Plan de Desarrollo Nacional.....	16
Tabla 3: Alineación con Plan decenal de Salud Pública	16
Tabla 4: Plan de Desarrollo Distrital.....	17
Tabla 5: Alineación de los Planes Estratégicos	18
Tabla 6: Objetivos estratégicos Subred Norte	19
Tabla 7:Metas institucionales de la Subred Norte.....	22
Tabla 8:Tendencias Tecnológicas	23
Tabla 9: Procesos Estratégicos	24
Tabla 10: Procesos Misionales	24
Tabla 11:Procesos de Apoyo	24
Tabla 12: Procesos de Evaluación y Control Fuente:	24
Tabla 13: Alineación con los procesos Estratégicos.....	26
Tabla 14: Alineación con los procesos misionales.....	27
Tabla 15: Alineación con los procesos de apoyo.....	29
Tabla 16: Alineación con los procesos de evaluación y control.....	29
<i>Tabla 17: Evaluar la criticidad de los activos de información.....</i>	<i>36</i>
Tabla 18: Plan de trabajo Gestión de Riesgo de seguridad y privacidad de la información	42

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 4 de 43 FECHA: 31/12/2022

1. INTRODUCCIÓN

La gestión de riesgos de seguridad y privacidad de la información, es un proceso estructurado que comprenden la identificación de activos, identificación de riesgos, valoración, evaluación y gestión de los posibles riesgos que se puedan presentar en las organizaciones y de esta forma ayudan a reducir la pérdida de la confidencialidad, integridad y disponibilidad de los activos de información brindando protección a los mismos y de esta forma permitiendo conocer las debilidades que pueden dificultar la buena gestión para el cumplimiento de los objetivos estratégico.

Por lo anterior y con el fin de dar cumplimiento a los lineamientos establecidos en el Decreto 612 de 2018 y al Modelo Integrado de Planeación y Gestión - MIPG, la Subred de Servicios de Salud Norte ESE elabora el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el cual permite orientar y dar lineamientos para la protección de Activos de Información ante los riesgos que atenten contra la Confidencialidad, Integridad y Disponibilidad a través de la implementación de medidas y controles de seguridad que permitan mitigar los riesgos e impactos a los que están expuestos, aprovechando los recursos de mejor manera y aportando el mayor valor a la operación de la Subred.

El presente Plan de Tratamiento de riesgos se encuentra articulado con la metodología de riesgos establecida en la Política de Administración de Riesgos de la Subred Norte ESE y las Guía 5 aprobada por el DAFP y MINTIC.

2. JUSTIFICACIÓN

En los últimos días la gestión de riesgos se ha transformado en uno de los procesos más relevantes en las entidades, permitiendo así identificar las posibles amenazas y vulnerabilidades que puedes afectar o causar daños a los activos de información, dando como resultado el análisis de las actividades y acciones tendientes a atacar dichas amenazas y vulnerabilidades, con el fin de evitar la posible materialización del riesgo y se cuente con procedimientos, guías, protocolos, etc., para poder actuar oportunamente ante dichas materializaciones.

Por lo cual, para la Subred de Servicios de Salud Norte ESE, es muy importante contar con un plan de gestión de riesgos de seguridad y privacidad de la información para el desarrollo de las actividades y tener un análisis óptimo para apoyar la continuidad de las operaciones.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Subred de Servicios de Salud Norte ESE, se aplica para todos los procesos, de acuerdo con el modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura de TI y soporta transversalmente los otros habilitadores de la política de gobierno digital, seguridad de la información, arquitectura y servicios ciudadanos digitales.

El aporte que arroja el presente plan permite identificar el nivel de riesgo en que se encuentran los activos de información mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a todos los funcionarios

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 5 de 43
		FECHA: 31/12/2022

y/o servidores, contratistas, proveedores y particulares a seguir las respectivas políticas, normas y procedimientos referentes a la Seguridad y Privacidad de la información y recursos.

4. OBJETIVO

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Subred de Servicios de Salud Norte ESE, mediante la definición de lineamientos, metodologías y actividades, con el fin de contar con una guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información.

5. MARCO NORMATIVO

5.1 DE ORDEN NACIONAL

NORMA	CONTENIDO
Constitución Nacional	Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación con el Derecho de Habeas 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 1273 de 2009 (Delitos Cibernéticos)	“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”.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 6 de 43
		FECHA: 31/12/2022

NORMA	CONTENIDO
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	El Art. 236 Establece que cuando el fiscal tenga motivos razonables, para inferir que el indicado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a la policía la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. La aprehensión que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso.
Ley 1712 de 2014	sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Decreto 1080 de 2015, “por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura”, el cual establece las directrices para la calificación de información pública, y se establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental
Ley 2199 de 2022	Por medio de la cual se desarrolla el artículo 325 de la constitución política y se expide el régimen especial de la región metropolitana Bogotá - Cundinamarca
Directiva 05 de 2020	Orientaciones para la implementación de estrategias pedagógicas de trabajo académico en casa y la implementación de una modalidad de complemento alimentario para consumo en casa
Ley 1581 de 2012 (Habeas Data)	“Por la cual se dictan disposiciones generales para la protección de datos”. Esta Ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Resolución CRC 3067 de 2011 “Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones”	Esta Resolución establece en el artículo 2.3, que los PRST que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo. Para lo cual, deben informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls. Filtros antivirus y la prevención del spam, phishing, malware entre otros; no obstante, la responsabilidad de los PRST no cubre los equipos del cliente, puesto que los mismos son controlados directamente por el usuario del servicio. Adicionalmente, los PRST que ofrezcan acceso a internet deberán implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, en línea con los marcos de seguridad definidos por la UIT, en lo relativo a las recomendaciones pertenecientes a las series X.800, y en relación con los siguientes aspectos: autenticación (UIT X.805 y UIT X.811), acceso (UIT X.805 y UIT X.812), no repudio (UIT X.805 y UIT X.813), confidencialidad de datos (UIT X.805 y UIT X.814), integridad de datos (UIT X.805 y UIT X.815) y disponibilidad (UIT X.805). Finalmente se

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 7 de 43
		FECHA: 31/12/2022

NORMA	CONTENIDO
	establece, los PRST a través de redes móviles, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122.
Resolución 500 de 2021	Resolución expedida por MinTIC por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Resolución 746 de 2022	Resolución en la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” modificado mediante el Decreto 1008 de 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”, en el artículo 2.2.9.1.1.3. incluye la seguridad de la información entre los principios de la Política de Gobierno Digital, de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital. (Comunicaciones, 2018)
Decreto 612 de 2018	“Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado”.
ISO/IEC 27001:2013	Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información
ISO/IEC 27005:2018	Es la norma internacional que describe cómo realizar una evaluación de riesgos de seguridad de la información de acuerdo con los requisitos de ISO 27001. Las evaluaciones de riesgos son una de las partes más importantes del proyecto de cumplimiento de ISO 27001 de una organización.

5.2 DE ORDEN INTERNACIONAL

NORMA	CONTENIDO
Convenio sobre Ciberdelincuencia del Consejo de Europa	Conocido como el convenio sobre Cibercriminalidad de Budapest, mediante el cual se adopta una legislación que facilita la prevención de las conductas delictivas y contribuye con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas
Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la OEA	Mediante la cual se establece una estrategia integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario, para la creación de una cultura de la seguridad cibernética

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de Documentos No haga copias de este documento porque corre el riesgo de tener una versión desactualizada

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 8 de 43 FECHA: 31/12/2022

Decisión 587 de la Comunidad Andina	Por la cual se establecen los lineamientos de la Política de seguridad externa común andina.
Declaración de la Cumbre de Gales de la OTAN en 2014	En donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.

6. VOCABULARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

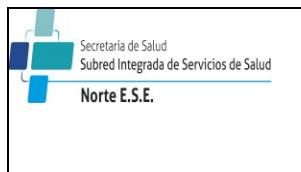
Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberspacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de Documentos. No haga copias de este documento porque corre el riesgo de tener una versión desactualizada.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 9 de 43 FECHA: 31/12/2022

interacción entre usuarios. (Resolución CRC 2258 de 2009).

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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 10 de 43 FECHA: 31/12/2022

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de recuperación de desastres

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
		Página 11 de 43
		FECHA: 31/12/2022

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad: Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

7. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

El presente Plan de tratamiento de riesgos se basa en la estructura y etapas definidas en el estándar internacional **ISO 27005:2018, ISO 27001:2013, la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública DAFP y el Modelo Nacional de Gestión de riesgos de la seguridad de la información** en Entidades públicas emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

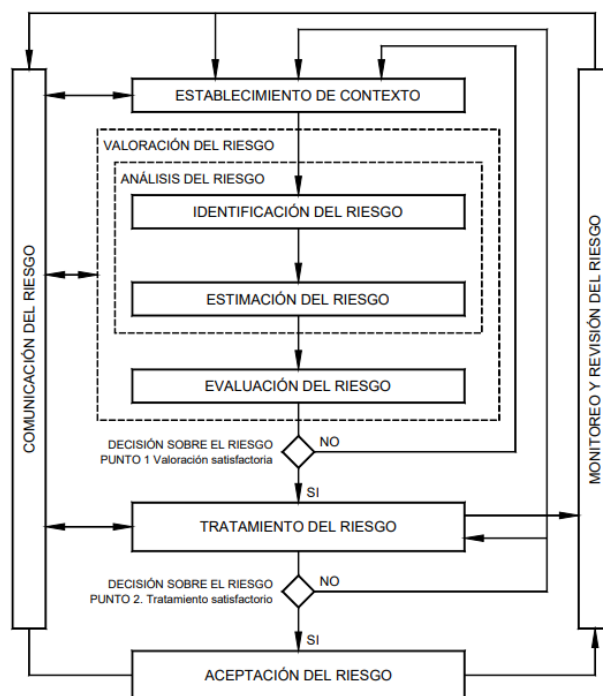
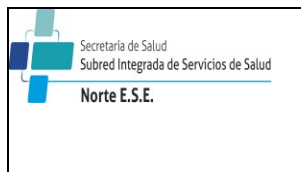
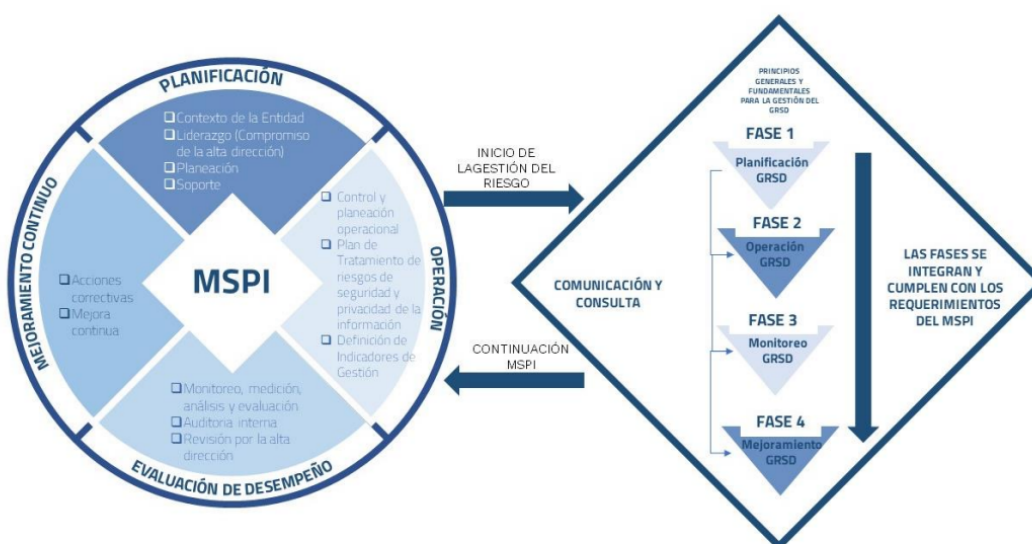


Ilustración 1: Proceso de gestión del riesgo en la seguridad de la información
(Fuente: Norma Técnica Colombiana NTC-ISO/IEC 27005)

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 12 de 43
		FECHA: 31/12/2022

El Proceso de gestión del riesgo dentro del Sistema de Gestión de Seguridad de la información, articula cada una de sus fases dentro del ciclo de planear, hacer, verificar y actuar (PHVA) mencionados en el Modelo de seguridad y privacidad de la información - MSPI, las cuales llevaran a cumplir las tareas requeridas para su funcionamiento:

Ilustración 2: Modelo de Privacidad y Seguridad de la Información Vrs Proceso de Gestión de Riesgos



(Fuente: Modelo nacional de gestión de riesgos de la seguridad de la información en la entidades públicas - MinTIC)

7.1 FASE DE PLANIFICACIÓN

La fase de planificación alcanza todo lo expuesto en los Pasos 1, 2 y 3 de la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública y contempla las siguientes actividades.

7.1.1 Identificación del Contexto

En esta primera etapa se define el alcance que tendrá la gestión de los Riesgos de seguridad y privacidad de la Información, los responsables y los criterios de evaluación de Riesgos que se identificaran y trataran.

Para la Subred de Servicios de Salud Norte ESE, la gestión de Riesgos de Seguridad y privacidad de la Información se realizará sobre los procesos, que tengan Activos de Información clasificados con criticidad Alta.

Los líderes de procesos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información. El Líder de Seguridad de la Información debe promover y apoyar la ejecución de esta actividad.

Conforme lo indica el DAFP, las entidades públicas deben realizar la identificación del contexto interno y externo de la

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 13 de 43
		FECHA: 31/12/2022

entidad, y en este caso para el análisis relacionado con seguridad de la información se dan lineamientos adicionales para realizar actividades conforme a los relacionado con seguridad digital

7.1.1.1 Contexto externo - motivadores estratégicos.

Esta sección del documento hace referencia a la identificación de los motivadores estratégicos a nivel nacional, territorial e institucional y los lineamientos y políticas que dan línea en la orientación y alineación la Estrategia de Tecnologías de la Información (PETI) de las entidades del País.

Alineación estratégica

Ilustración 3: Alineación Estratégica

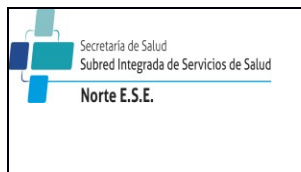


Fuente: Plan estratégico de tecnologías de la información - PETI

Tabla 1: Alineación Estratégica

Motivador	Fuente
Estrategia Nacional	- Objetivos de Desarrollo Sostenible - Plan Nacional de Desarrollo - Pacto por la Transformación Digital
Estrategia Sectorial	- Plan decenal de Salud pública - Plan de Desarrollo Distrital
Estrategia Institucional	- Plan Operativo Anual
Lineamientos y Políticas	- Transformación Digital - Política de Gobierno Digital - Modelo Integrado de Planeación y Gestión.

Fuente: Plan estratégico de tecnologías de la información - PETI

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 14 de 43 FECHA: 31/12/2022

Objetivos de Desarrollo Sostenible

En septiembre de 2015, más de 150 jefes de Estado y de Gobierno se reunieron en la histórica Cumbre del Desarrollo Sostenible en la que aprobaron la Agenda 2030. Esta Agenda contiene 17 objetivos de aplicación universal que, desde el 1 de enero de 2016, rigen los esfuerzos de los países para lograr un mundo sostenible en el año 2030.

Los Objetivos de Desarrollo Sostenible (ODS) son herederos de los Objetivos de Desarrollo del Milenio (ODM) y buscan ampliar los éxitos alcanzados con ellos, así como lograr aquellas metas que no fueron conseguidas.

Estos nuevos objetivos presentan la singularidad de instar a todos los países, ya sean ricos, pobres o de ingresos medianos, a adoptar medidas para promover la prosperidad al tiempo que protegen el planeta. Reconocen que las iniciativas para acabar con la pobreza deben ir de la mano de estrategias que favorezcan el crecimiento económico y aborden una serie de necesidades sociales, entre las que cabe señalar la educación, la salud, la protección social y las oportunidades de empleo, a la vez que luchan contra el cambio climático y promueven la protección del medio ambiente.

A pesar de que los ODS no son jurídicamente obligatorios, se espera que los gobiernos los adopten como propios y establezcan marcos nacionales para su logro. Los países tienen la responsabilidad primordial del seguimiento y examen de los progresos conseguidos en el cumplimiento de los objetivos, para lo cual es necesario recopilar datos fiables, accesibles y oportunos. Las actividades regionales de seguimiento y examen se basarán en análisis llevados a cabo a nivel nacional y contribuirán al seguimiento y examen a nivel mundial.

Se establecieron 17 Objetivos, los cuales se describen a continuación:



Ilustración 4 Objetivos de Desarrollo Sostenible
Fuente: Plan estratégico de tecnologías de la información - PETI

Desde hace tiempo se reconoce que para conseguir una economía robusta se necesitan inversiones en infraestructura. Las inversiones en infraestructura (transporte, energía, comunicaciones, etc.) son fundamentales para lograr un desarrollo sostenible, empoderar a las sociedades de numerosos países, fomentar una mayor estabilidad social y conseguir ciudades más resistentes al cambio climático.

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de Documentos. No haga copias de este documento porque corre el riesgo de tener una versión desactualizada.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 15 de 43 FECHA: 31/12/2022

Además de los fondos gubernamentales y de la asistencia oficial para el desarrollo, también se está promoviendo la inversión del sector privado para los países que necesitan recursos financieros y tecnológicos.

El Objetivo 9 busca Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación; contemplando en una de sus metas:

- Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020.

Plan de Desarrollo de la Nación

En el libro 1 /Numeral 2/ Objetivos y estrategias del Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, pacto por la equidad, Pactos transversales: VII. Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento.

OBJETIVO	NUMERAL	ITEM
Objetivo 3. Articular todos los agentes del sector salud en torno a la calidad	e) Incentivar herramientas que pongan a disposición información de calidad y desempeño de cara a los usuarios para empoderarlos en la toma de decisiones	• MINSALUD promoverá la modernización de la gestión de prestación de servicios a través de avances en la interoperabilidad de los sistemas de información y mejoras en conectividad en los territorios apartados, en articulación con los lineamientos de MinTIC (impulsando los programas de telesalud, historia clínica electrónica interoperable, factura electrónica y demás apropiaciones TIC) y en el marco de los Servicios Ciudadanos Digitales. • Se desarrollará el marco jurídico que asegure el flujo de información dentro del Sistema de Seguridad Social Integral, para garantizar la prestación de los servicios asociados al mismo, armonizando la normatividad relativa a la política nacional de explotación de datos, protección de datos personales y seguridad digital que rigen la materia.
	f) Incentivar la investigación en salud	• Se promoverán y apoyarán proyectos que aporten a la innovación, investigación y desarrollo en prestación de servicios; o modelos de salud que apuesten a la transformación tecnológica del sector, en articulación con los lineamientos de MinTIC y en el marco de los Servicios Ciudadanos Digitales.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 16 de 43 FECHA: 31/12/2022

OBJETIVO	NUMERAL	ITEM
4) Objetivo 4. Lograr más infraestructura y dotación en salud, como soporte al acceso efectivo y la calidad	a) Instituciones prestadoras de servicios de salud dotadas con infraestructura adecuada y capacidad para responder con calidad y efectividad a las necesidades de toda la población	Se implementará un plan de acción inmediato para los hospitales públicos, con el fin de identificar las necesidades en infraestructura, dotación, calidad, talento humano y sostenibilidad. Se aplicará un modelo diferencial de acuerdo con las necesidades identificadas y la priorización que defina Min Salud.

Tabla 2: Plan de Desarrollo Nacional
Fuente: Plan estratégico de tecnologías de la información - PETI

Plan Decenal de Salud

En el Plan Decenal de Salud Pública PDSP 2012-2021 se plantea la línea de trabajo para dar respuesta a los desafíos actuales en salud pública y para consolidar, en el marco del sistema de protección social, las capacidades técnicas en los ámbitos nacional y territorial para la planeación, ejecución, seguimiento y evaluación de las intervenciones, de acuerdo con los Objetivos de Desarrollo del Milenio (ONU, 2000).

DIMENSIONES GENERALES	DIMENSIÓN ESPECÍFICA	COMPONENTE
Dimensiones prioritarias	2. Vida saludable y condiciones no transmisibles	b. Condiciones crónicas prevalentes: tecnologías apropiadas para la promoción y la atención integral.
	3. Convivencia social y salud mental	a. Promoción de la salud mental y la convivencia: uso de tecnologías de la información y las comunicaciones en pro de la salud mental.
	5. Sexualidad, derechos sexuales y reproductivos	b. Prevención y atención integral en salud sexual reproductiva desde un enfoque de derechos: abordaje integral de las violencias de género y violencias sexuales, que incluye consolidación de sistemas de información, gestión articulada entre programas e instituciones y atención integral a víctimas.
Dimensiones transversales	1P5/1. Gestión diferencial de poblaciones vulnerables	a. Componente: Desarrollo integral de las niñas, niños y adolescentes: gerencia de las políticas públicas de primera infancia, infancia y adolescencia; estrategias de disminución de barreras de acceso a los servicios de salud; estrategias de tecnologías de la información y las comunicaciones al servicio de la salud. e. Componente: Discapacidad: articulación y gestión intersectorial para el acceso de la población con discapacidad al ámbito educativo, laboral, social, cultural, de participación ciudadana, a las tecnologías de la información y las comunicaciones.

Tabla 3: Alineación con Plan decenal de Salud Pública
Fuente: Plan estratégico de tecnologías de la información - PETI

Plan de Desarrollo Distrital

Plan de Desarrollo Distrital 2020-2024 “Un Nuevo Contrato Social y Ambiental Para El Siglo XXI”; dentro de su

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de Documentos. No haga copias de este documento porque corre el riesgo de tener una versión desactualizada.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 17 de 43
		FECHA: 31/12/2022

estructura contiene en Artículo 13. Dentro de su estructura tiene 5 propósitos, 30 logros de la ciudad y 70 programas generales.

PROPÓSITO	LOGRO DE LA CIUDAD	PROGRAMA	ITEM
Propósito 1: Hacer un nuevo contrato social con igualdad de oportunidades para la Inclusión social, productiva y política.	Completar la implementación de un modelo de salud con enfoque poblacional- diferencial, de género, participativo, resolutorio y territorial que aporte a la modificación de los determinantes sociales de la salud.	Mejora de la gestión de instituciones desalud.	2024 cumplir con el 100% en la implementación de la arquitectura empresarial de soluciones que integran exitosamente la mejora de los procesos estratégicos, técnicos y operativos de la Dirección Territorial de Salud. A 2024 el sector salud contará con una infraestructura y dotación que le permita prestar servicios con calidad y oportunidad acorde con el Modelo de Salud basado en el enfoque poblacional, diferencial, participativo, resolutorio y territorial.
			A 2024 mantener por encima del 95% la interoperabilidad de la Historia Clínica Electrónica en las 4 subredes de servicios de salud y avanzar en los puntos de la red privada priorizados.
Propósito 5: Construir Bogotá Región con gobierno abierto, transparente y ciudadanía Consciente.	Posicionar al Gobierno Abierto de Bogotá-GABO como una nueva forma de gobernanza que reduce el riesgo de corrupción e incrementa el control ciudadano del gobierno	Gobierno Abierto	A 2024, diseñar e implementar la Estrategia de Gobierno Abierto en salud de Bogotá D.C. (GABO), a través de acciones de participación social en salud, transparencia, control social y rendición de cuentas.
	Posicionar globalmente a Bogotá como territorio inteligente (Smart City)	Transformación digital y gestión de TIC para un territorio inteligente	A 2024 diseñar e implementar la Estrategia de Transformación Digital en Salud

Tabla 4: Plan de Desarrollo Distrital.

Fuente: Plan estratégico de tecnologías de la información - PETI

Alineación Planes Estratégicos

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 18 de 43
		FECHA: 31/12/2022

	ESTRATEGIA NACIONAL	ESTRATEGIA SECTORIA	DISTRITAL	INSTITUCIONAL
	Min Salud promoverá la modernización de la gestión de prestación de servicios a través de avances en la interoperabilidad de los sistemas de información y mejoras en conectividad en los territorios apartados, en articulación con los lineamientos de MinTIC (impulsando los programas de telesalud, historia clínica electrónica interoperable, factura electrónica y demás apropiaciones TIC) y en el marco de los Servicios Ciudadanos Digitales.	b. Prevención y atención integral en salud sexual reproductiva desde un enfoque de derechos: abordaje integral de las violencias de género y violencias sexuales, que incluye consolidación de sistemas de información, gestión articulada entre programas e instituciones y atención integral a víctimas.	A 2024 mantener por encima del 95% la interoperabilidad de la Historia Clínica Electrónica en las 4 subredes de servicios de salud y avanzar en los puntos de la red privada priorizados.	Implementar el módulo de inteligencia de negocios del sistema de información Servinte Clinical Suite acorde con un plan de trabajo.
	Se implementará un plan de acción inmediato para los hospitales públicos, con el fin de identificar las necesidades en infraestructura, dotación, calidad, talento humano y sostenibilidad. Se aplicará un modelo diferencial de acuerdo con las necesidades identificadas y la priorización que defina MinSalud.	b. Condiciones crónicas prevalentes: tecnologías apropiadas para la promoción y la atención integral.	A 2024 el sector salud contará con una infraestructura y dotación que le permita prestar servicios con calidad y oportunidad acorde con el Modelo de Salud basado en el enfoque poblacional, diferencial, participativo, resolutivo y territorial.	

Tabla 5: Alineación de los Planes Estratégicos
Fuente: Plan estratégico de tecnologías de la información - PETI

7.1.1.2 Contexto Institucional

Misión

Somos una Empresa Social del Estado innovadora y socialmente responsable, que presta servicios de salud integrales y de calidad, con participación activa en la formación de talento humano y desarrollo de la docencia y la investigación, contribuyendo al mejoramiento de la calidad de vida de la población.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 19 de 43
		FECHA: 31/12/2022

Visión

Para el 2030, la Subred Norte será reconocida como la Empresa Social del Estado, líder en la prestación de servicios asistenciales de excelencia, centrada en la persona, con atención humanizada, a través de la formación del recurso humano asistencial y administrativo de alta calidad, inspirada por la investigación y el desarrollo. Tendremos un modelo de gestión económico, ambientalmente sostenible, generador de equidad y legitimidad social.

Objetivos Estratégicos

ID	Objetivo
A. MODERNIZACIÓN EMPRESARIAL DE LA SUBRED NORTE E.S.E. PERSPECTIVA	
001	Fortalecer la línea de gestión empresarial operacional - Productividad
002	Desarrollar línea de gestión institucional - Competitividad
003	Desarrollar línea de gestión ambiental - Sostenibilidad
B. PERSPECTIVA FINANCIERA	
004	Lograr la sostenibilidad financiera de la Subred Norte
C. PERSPECTIVA CLIENTES	
005	Incrementar nivel de fidelización y satisfacción de los usuarios
006	Desarrollar línea de gestión social - Legitimidad
007	Diversificación portafolio de servicios
008	Incrementar portafolio de clientes
D. PERSPECTIVA PROCESOS	
009	Alcanzar estándares superiores de calidad en salud
010	Implementar sistemas integrales de gestión en la Subred Norte
E. PERSPECTIVA DE INNOVACIÓN Y APRENDIZAJE	
011	Generar y difundir crecimiento científico en salud
012	Fortalecer competencias del Talento Humano con énfasis en docentes y estudiantes
013	Fortalecer el sistema de información y comunicaciones

Tabla 6: Objetivos estratégicos Subred Norte

Fuente: Plan estratégico de tecnologías de la información - PETI

Indicadores plan de desarrollo institucional

ID	META	LÍNEA BASE
001	Implementar al 100% el aplicativo de semaforización incluidos los indicadores trazadores (PDD)	No Existe
002	Ejecutar al 100% un programa de atención a brotes en salud pública. (PDD)	Covid-19
003	Desplegar una estrategia a través de equipos interdisciplinarios para el abordaje del 100% de las acciones PSPIC. (PTS)	Existe por PSPIC
004	Mejorar los indicadores trazadores en un 1%, para optimizar la capacidad instalada mejorando la producción de los servicios asistenciales, hospitalarios, ambulatorios, complementarios, urgencias y de gestión del riesgo. (DF)	Existe por servicios

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 20 de 43
		FECHA: 31/12/2022

ID	META	LÍNEA BASE
005	Incrementar la contratación de servicios de salud a través de la EAPB así (DF): • Unidad ejecutora o Funcional Unidad de quemados 41.799.493.419 Continuidad de la Unidad ejecutora APH, el costo fue proyectado 60.901.311.870 • Incrementar la oferta de servicios de grupos • quirúrgicos del 5% para todos los pagadores 3.887.816.976	Existe histórico de contratación
006	Implementar el 100% de las RIAS priorizadas (PTS)	9 RIAS
007	Implementar al 100% la automatización del laboratorio en la UMHEs Simón Bolívar y la puesta en marcha del laboratorio de biología molecular en la UMHEs calle 80, buscando mejorar los tiempos de operación con miras a la mejora de la oportunidad.	No Existe
008	Cumplir al 100% con los proyectos inscritos en el Plan Bienal de Inversión y aprobados por la SDS (infraestructura y dotación).(PDD)	9 proyectos inscritos en BPIN
009	Ejecutar en un 80% el PINAR (<i>incluye disminuir en 90% el consumo de papel en los servicios asistenciales y administrativos</i>).	porcentaje de ejecución: 74%
010	Implementar al 25% el hospital verde en la Subred Norte (PDD)	Existe por unidad
011	Recaudar sobre la facturación de la vigencia por año, ascendente así (DF): 2020 72%; 2021 76%; 2022 80%; 2023 86%. Aplica para cada vigencia IPC +2% vía tarifa	Informe de gestión financiera
012	Reducir gastos asociados a la nómina así (DF): 3,5% de la nómina 5% horas extras y recargos 20% personal administrativo 2% de la contratación de OPS	Ver informe Costos 2020
013	Reducir en 3% (\$897.695.159) servicios públicos. (DF)	Existe por unidad
014	Cambiar la tercerización imágenes diagnósticas por prestación directa de servicios (ahorro de: \$8.258.689.158). (DF)	No Existe
015	Fortalecer en 5% el ingreso proveniente de stakeholders con beneficio público	No Existe
016	Incrementar al 96% el índice de satisfacción del usuario	Indicador 2020 Satisfacción del usuario 95%
017	Diseñar e implementar una (1) Estrategia de Gestión Territorial en Salud orientada a fortalecer los procesos comunitarios e intersectoriales en la Subred Norte (PTS)	No Existe

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 21 de 43
		FECHA: 31/12/2022

ID	META	LÍNEA BASE
018	Diseñar e implementar al 75% la estrategia de cuidado a la ciudadanía. (PDD)	Informe PSPIC
019	Implementar el 100% del programa de organización, integralidad e integración de servicios especializados en cada una de las UMHEs de la Subred Norte.	No Existe
020	Actualizar al 100% el portafolio de servicios institucional de acuerdo a los servicios ofertados. (DF)	Por Actualizar
021	Elaborar e implementar al 70% el plan de comunicaciones para la divulgación de los servicios ofertados, midiendo los resultados obtenidos, frente a la expansión, apertura y adherencia de servicios	No Existe
022	Habilitar servicios ajustados a tipología de portafolios y acreditar 3 unidades de servicios de salud así USS UMHEs Engativá, CAPS Chapinero y Boyacá Real. (DF)	No Existe
023	Mejorar en 10% la capacidad académica de acuerdo a la capacidad instalada ofertada, a través de convenios de docencia y servicios.	Capacidad académica 2020 I semestre 48%
024	Implementar el 50% de la arquitectura empresarial desoluciones (PTS).	No Existe
025	Incrementar en 15% el número de colaboradores sensibilizados en la cultura de seguridad del paciente y humanización a través de la capacitación al personal asistencial.	Informe humanización
026	Implementar en un 80% la contratación digital utilizando herramientas tecnológicas que disminuyan la firma física de documentos, contribuyendo a la política de cero papel	No Existe
027	Diseñar e implementar herramientas que garanticen la apropiación de una cultura de autocontrol	No Existe
028	Fortalecer ingreso proveniente del CIS-Norte en \$826.919.695 (DF)	No Existe
029	Certificar a la Subred Norte en buenas prácticas clínicas (UdeA)	Informe Gestión del Conocimiento
030	Implementar el 100% de las estrategias de habilitación y acreditación, necesarias para incluir un hospital universitario en el portafolio de servicios. (PDD)	No Existe
031	Ejecutar el 100% del programa de salud mental integral en la Subred Norte (PDD)	Programa Conscientemente
032	Programa de inducción y reinducción	
033	Cubrir el 100% de las vacantes asignadas y crear el 100% de empleos temporales asignados a la Subred Norte. (PDD)	Informe de Talento Humano
034	Implementar al 95% el intercambio recíproco de la información en la historia clínica (PDD)	No Existe

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 22 de 43
		FECHA: 31/12/2022

ID	META	LÍNEA BASE
035	Diseñar, desarrollar e implementar la agenda estratégica digital, que incluya áreas de infraestructura, conectividad, facturación electrónica, digitalización desoportes, historia clínica electrónica. (PDD)	No Existe

Tabla 7: Metas institucionales de la Subred Norte

Fuente: Plan estratégico de tecnologías de la información - PETI

Tendencias tecnológicas

NOMBRE	DESCRIPCIÓN
Uso de nube- Plataforma como servicio	Plataforma de correo en la nube para garantizar confiabilidad y almacenamiento escalable
Automatización de procesos con motor RPA (Robotic Process Automation)	Robotización de procesos administrativos y trámites que tengan actividades repetitivas susceptibles de automatización, mejorando los tiempos de respuesta hacia el cliente final
Software para análisis de datos descriptivo	Aplicativo que permita a partir un conjunto de datos realizar su análisis descriptivo facilitando la identificación de características de la data que permitan ajustar los procesos
Software para análisis de datos predictivo	Aplicativo que permita a partir un conjunto de datos realizar su análisis predictivo facilitando la identificación de tendencias que permitan ajustar los procesos
Software de inteligencia artificial	Aplicativo que permita a partir un conjunto de datos aplicar algoritmos de inteligencia artificial facilitando la identificación de clasificación y regresión de nuevos datos que permitan ajustar los procesos
Blockchain	Control y trazabilidad en las cadenas de abastecimiento en los trámites de la entidad
Gestión y análisis de datos estructurados (Motores ETL-ELT, Bodegas de datos y datamarts)	Consolidación de las diferentes fuentes de información de la entidad en un único repositorio que facilite la consulta centralizada de información
Plataforma colaborativa	Aplicativo que facilite la comunicación multimedial entre el personal de los procesos permitiendo la trazabilidad, almacenamiento y seguimiento de las comunicaciones
Internet de las cosas (IOT)	Plataforma que permita la gestión e interconectividad entre los dispositivos de monitoreo, sensores y biomédicos con capacidades de conectividad cableada o wifi a la red, facilitando la recolección y centralización de los datos generados
Arquitectura de sistemas orientada a Microservicios	Plataforma que permita la migración y gestión de servicios monolíticos a microservicios en el caso de aplicaciones web como la intranet, aprovechando de manera eficiente y escalable la actual infraestructura de virtualización
Máquinas virtuales (Virtualización de hardware)	Fortalecer la actual infraestructura de virtualización en VMware

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 23 de 43
		FECHA: 31/12/2022

NOMBRE	DESCRIPCIÓN
Virtualización de sistema operativo en contenedores (Docker)	Plataforma que permita la migración y gestión de servicios monolíticos a microservicios en el caso de aplicaciones web como la intranet, aprovechando de manera eficiente y escalable la actual infraestructura de virtualización
Metodologías ágiles	Mejorar la calidad de los desarrollos propios de la institución
Devops	Automatizar el control, monitoreo, implementación y cambio de la infraestructura informática de la institución

Tabla 8: Tendencias Tecnológicas

Fuente: Plan estratégico de tecnologías de la información - PETI

7.1.2 Modelo Operativo de Procesos

A continuación, se describe la estructura del mapa de procesos de la entidad, el cual representa el comportamiento de ésta, dando orientación a cómo se gestionan las actividades para dar cumplimiento a sus objetivos y metas estratégicas.



Ilustración 4: Mapa de procesos institucional

Fuente: <https://www.subrednorte.gov.co/transparencia/informacion-entidad/mapa-procesos> Fecha: 19 de diciembre de 2022

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 24 de 43 FECHA: 31/12/2022

7.1.2.1 Descripción de los procesos

Procesos estratégicos

Nombre de procesos	Objetivo
Gestión estratégica	Se enfoca en las definir las políticas, estrategias y líneas de acción generales para el direccionamiento de la entidad. De acuerdo con la anterior, se definieron en la Subred Integrada de Servicios de Salud Norte ESE, dentro de este grupo cuatro procesos
Participación social y atención al usuario	
Docencia e investigación	
Gestión de calidad	

Tabla 9: Procesos Estratégicos

Fuente: Plan estratégico de tecnologías de la información - PETI

Procesos misionales

Nombre de procesos	Objetivo
Gestión del riesgo en salud	El macroproceso misional se centra en generar valor durante el proceso de atención a nuestros usuarios, incidiendo directamente en su satisfacción. Para este efecto se definieron cinco procesos con sus correspondientes procedimientos.
Gestión ambulatoria	
Gestión de urgencias	
Gestión de hospitalización y cirugía	
Gestión de servicios complementarios	

Tabla 10: Procesos Misionales

Fuente: Plan estratégico de tecnologías de la información - PETI

Procesos de apoyo

Nombre de procesos	Objetivo
Gestión financiera	En el macroproceso de apoyo se enmarcan las actividades relacionadas con la entrega a los diferentes procesos de los recursos necesarios en cuanto a personas, maquinaria y materia prima, para poder generar el valor agregado y la satisfacción del usuario. La Subred Norte ESE definió seis procesos.
Gestión de la contratación	
Gestión jurídica	
Gestión TICS	
Gestión del ambiente físico y tecnológico	
Gestión del talento humano	

Tabla 11: Procesos de Apoyo

Fuente: Plan estratégico de tecnologías de la información - PETI

Procesos de evaluación y control

Nombre de procesos	Objetivo
Evaluación de gestión	El grupo de procesos de evaluación permite generar los controles y mejoras al sistema de gestión.
Gestión disciplinaria	

Tabla 12: Procesos de Evaluación y Control Fuente:

Plan estratégico de tecnologías de la información - PETI

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 25 de 43 FECHA: 31/12/2022

7.1.2.2 Alineación de TI con los procesos

En el siguiente cuadro se presenta la alineación de los recursos de soporte de TI con los procesos más representativos de acuerdo con los objetivos institucionales, las estrategias de TI y el mapa de procesos de la Entidad.

ID	Proceso	Categoría	Sistema de Información
1	Gestión estratégica	Estratégicos	Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
2	Participación social y atención al usuario		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
3	Docencia e investigación		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Moodle
		Sistema de gestión documental ORFEO	
		ZIMBRA	

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 26 de 43 FECHA: 31/12/2022

ID	Proceso	Categoría	Sistema de Información
4	Gestión de calidad		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA

Tabla 13: Alineación con los procesos Estratégicos
Fuente: Plan estratégico de tecnologías de la información - PETI

ID	Proceso	Categoría	Sistema de Información
5	Gestión del riesgo en salud	Misional	Mesa de servicios GLPI
			Voz IP
			Moodle
			Sistema de Gestión Documental ORFEO
			Correo institucional Outlook 365
			Internet/Intranet
			Portal WEB
			ZIMBRA
6	Gestión ambulatoria		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 27 de 43 FECHA: 31/12/2022

ID	Proceso	Categoría	Sistema de Información
7	Gestión de urgencias		Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise
8	Gestión de hospitalización y cirugía		Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise
9	Gestión de servicios complementarios		Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise

Tabla 14: Alineación con los procesos misionales
Fuente: Plan estratégico de tecnologías de la información - PETI

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 28 de 43
		FECHA: 31/12/2022

ID	Proceso	Categoría	Sistema de Información
10	Gestión financiera	Apoyo	Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Portal WEB
			Voz IP
			Mesa de servicios GLPI
			Servinte Clinical Suite Enterprise
11	Gestión de la contratación		Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Portal WEB
			Voz IP
			Mesa de Servicios
			12
Sistema de Gestión Documental ORFEO			
Internet/Intranet			
Correo institucional Outlook 365			
Portal WEB			
Voz IP			
Mesa de Servicios			
13	Gestión TICS		
			Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Mesa de servicios GLPI
			Portal WEB
			Voz IP
			Gestión Dispositivos
			Servinte Clinical Suite Enterprise
14	Gestión del ambiente físico ytecnológico		Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Mesa de servicios GLPI
			Voz IP
			Portal WEB
			15
Sistema de Gestión Documental ORFEO			
Internet/Intranet			
Correo institucional Outlook 365			
Portal WEB			
Voz IP			
Correo electrónico ZIMBRA			
Mesa de servicios GLPI			

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 29 de 43 FECHA: 31/12/2022

ID	Proceso	Categoría	Sistema de Información
			Sinergy
			Mesa de Servicios

Tabla 15: Alineación con los procesos de apoyo
Fuente: Plan estratégico de tecnologías de la información - PETI

ID	Proceso	Categoría	Sistema de Información
16	Evaluación de gestión	Evaluación y Control	Sistema de Gestión Documental ORFEO
			Correo electrónico ZIMBRA
			Correo institucional Outlook 365
			Internet/Intranet
			Voz IP
			Portal WEB
			Mesa de servicios GLPI
17	Gestión disciplinaria		Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Correo institucional Outlook 365
			Voz IP
			Mesa de servicios GLPI
			Internet/Intranet
			Portal WEB

Tabla 16: Alineación con los procesos de evaluación y control
Fuente: Plan estratégico de tecnologías de la información - PETI

7.1.2.3 Alineación de MSPI con el Estándar de Gerencia de la Información

A continuación, se presenta los estándares de Gerencia de la Información relacionados con el Modelos de Seguridad y privacidad de la información:

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 30 de 43
		FECHA: 31/12/2022

GRUPO DE ESTANDARES	ESTANDAR	ESTÁNDAR / CRITERIO AFECTADO
Estándares de Gerencia de la Información	Estándar 143. Código: (GI2)	Existe un proceso para planificar la gestión de la información en la organización; este proceso está documentado, implementado y evaluado en un plan de gerencia de la información, e incluye: - La identificación de las necesidades de información. - Un proceso de implementación basado en prioridades. - La recolección sistemática y permanente de la información necesaria y relevante que permita a la dirección y a cada uno de los procesos, la toma oportuna y efectiva de decisiones. - Flujo de la información. - Minería de datos. - Almacenamiento, conservación y depuración de la información. - Seguridad y confidencialidad de la información. - Uso de la información. - El uso de nuevas tecnologías para el manejo de la información. - Recolección sistemática de las necesidades, las opiniones y los niveles de satisfacción de los clientes del sistema de información. - Cualquier disfunción en el sistema de información es recolectada, analizada y resuelta. - La información soporta la gestión de los procesos relacionados con la atención al cliente de la organización. - Identificación de espacios gerenciales y técnicos para el análisis de la información. - Definición de indicadores corporativos que incluyan: Seguridad del paciente, humanización, gestión del riesgo y gestión de la tecnología. - Comparación con mejores prácticas. - Sistema de medición, evaluación y mejoramiento del plan.
	Estándar 146. Código: (GI5)	Existen mecanismos estandarizados, implementados y evaluados para garantizar la seguridad y confidencialidad de la información - La seguridad y la confidencialidad. - Acceso no autorizado. - Pérdida de información. - Manipulación. - Mal uso de los equipos y de la información, para fines distintos a los legalmente contemplados por la organización. - Deterioro, de todo tipo, de los archivos. - Los registros médicos no pueden dejarse o archivarse en sitios físicos donde no esté restringido el acceso a visitantes o personal no autorizado. - Existe un procedimiento para la asignación de claves de acceso. - Existencia de backups y copias redundantes de información. - Control documental y de registros. - Indicadores de seguridad de la información.
	Estándar 147. Código: (GI6)	Existe un mecanismo definido implementado, evaluado y formal para transmitir los datos y la información. La transmisión garantiza: - Oportunidad. - Facilidad de acceso. - Confiabilidad y validez de la información. - Seguridad. - Veracidad. Oportunidad. - Facilidad de acceso. - Confiabilidad y validez de la información. - Seguridad. - Veracidad.
	Estándar 148. Código: (GI7)	Existen procesos para la gestión y minería de los datos, que permitan obtener la información en forma oportuna, veraz, clara y conciliada. Esto incluye: - La transmisión del dato. - La definición de responsables de cada paso en la gestión del dato. - Los permisos asignados a cada responsable. - La validación y la conciliación entre los datos recolectados y gestionados en forma física y/o electrónica.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 31 de 43
		FECHA: 31/12/2022

GRUPO DE ESTANDARES	ESTANDAR	ESTÁNDAR / CRITERIO AFECTADO
		La generación de información útil en los niveles operativos. La evaluación de la calidad y coherencia de datos generados.
	Estándar 150. Código: (GI9)	La gestión de la información relacionada con los registros clínicos, sea en medio físico o electrónico, garantiza la calidad, la seguridad y la accesibilidad de los mismos. Incluye: Orden. Legibilidad y concordancia clínico-patológica. Claridad y actualización de los registros clínicos. Adecuado archivo de los registros clínicos y fácil disponibilidad cuando sean requeridos. Auditoría sistemática y periódica a la calidad de forma y contenido de los registros clínicos. Garantía de la custodia de los registros clínicos. Unicidad de los registros clínicos para cada usuario. Sistema de identificación y numeración unificado para todos los registros clínicos. Esquema del proceso de transición a historia clínica electrónica. Sistemas de chequeo para evitar errores en la identificación de los usuarios. Sistemas de alarma redundante para las condiciones que lo ameriten. Procesos para la entrega de los resúmenes de historia clínica solicitados por las autoridades competentes o los mismos usuarios. La organización garantiza que en los procesos de la gerencia de información es posible verificar si el usuario ha asistido previamente a la institución, en qué fechas, qué profesional lo ha atendido, qué exámenes se le han ordenado, etc. Cuando se tenga un sistema mixto de registro de atenciones (electrónico y manual), se debe garantizar que haya un solo sistema de identificación del paciente, para que el contenido de las atenciones esté disponible para cualquier prestador y se le pueda hacer auditoría integral al registro.
	Estándar 155. Código: (GIMCC1)	La gestión de las oportunidades de mejora consideradas en el proceso organizacional de mejoramiento continuo, que apliquen al grupo de estándares, se desarrolla teniendo en cuenta: El enfoque organizacional del mejoramiento continuo. La implementación de oportunidades de mejora priorizadas y la remoción de barreras de mejoramiento, por parte de los equipos de autoevaluación, los equipos de mejora y los demás colaboradores de la organización." La articulación de oportunidades de mejora que tengan relación entre los diferentes procesos y grupos de estándares. El seguimiento a los resultados del mejoramiento, la verificación del cierre de ciclo, el mantenimiento y el aseguramiento de la calidad. La comunicación de los resultados.
	Estándar 151. Código: (GI10)	Existe un plan de contingencia diseñado, implementado y evaluado que garantice el normal funcionamiento de los sistemas de información de la organización, sean manuales, automatizados, o ambos. Cualquier disfunción en el sistema es recolectada, analizada y resuelta. Lo anterior incluye mecanismos para prevenir eventos adversos relacionados con el manejo de los sistemas de información en especial alarmas en historia clínica.

7.1.3 Estructura organizacional

La subred integrada de servicios de salud norte ESE, para el cumplimiento de su misión establece la siguiente estructura orgánica:

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 32 de 43 FECHA: 31/12/2022

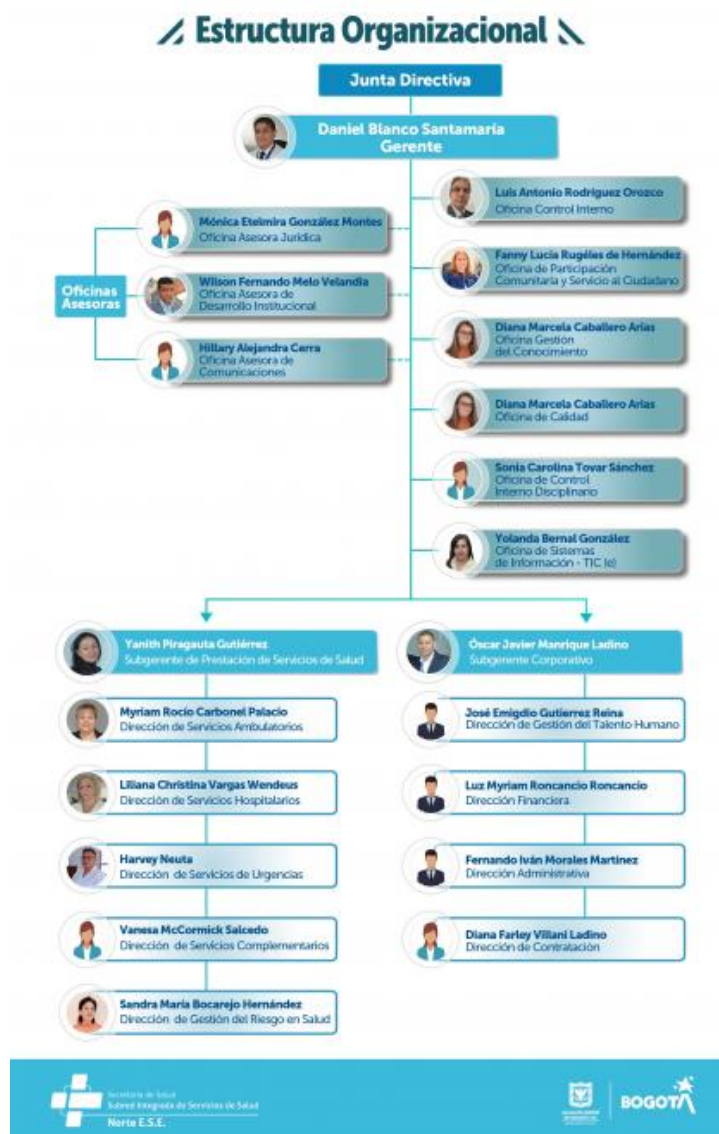


Ilustración 5: Estructura orgánica institucional

Fuente: <https://www.subrednorte.gov.co/transparencia/informacion-entidad/organigrama>, Fecha: 19 de diciembre de 2022

7.1.4 Política de Gestión de Administración de Riesgos de la Subred Integrada de Servicios de Salud Norte E.S.E

Enunciado:

La Subred Integrada de Servicios de Salud Norte E.S.E, se compromete a adoptar los mecanismos y acciones necesarias para una eficaz administración de sus riesgos, de tal forma que se prevengan o minimicen sus impactos, mediante una adecuada identificación, análisis, valoración, priorización y control, orientados a garantizar la integridad, seguridad y la calidad en el desarrollo de sus actividades y la prestación de sus servicios.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 33 de 43
		FECHA: 31/12/2022

Objetivo de la política de gestión de administración de riesgos:

Promover la implementación de metodologías que permitan la articulación del sistema de gestión de riesgo institucional con el fin de alcanzar niveles aceptables de riesgos residuales para poder cumplir los objetivos misionales, estratégicos y de procesos con participación activa de los colaboradores y de acuerdo a los niveles de responsabilidad establecida en las líneas de defensa acorde con la Política de Atención Integral en Salud y su modelo de atención

- Establecer estrategias eficaces de control para los riesgos de mayor impacto para la entidad
- Promover el seguimiento oportuno a las acciones establecidas para la mitigación de los riesgos identificados
- Promover mecanismos orientados a fomentar el conocimiento en la gestión del riesgo en todos los colaboradores de la entidad
- Reforzar la autorregulación de los procesos institucionales, con participación activa de los colaboradores y de acuerdo a la responsabilidad establecida en las líneas de defensa

Alcance de la política de gestión de administración de riesgos:

La política de gestión de administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de **seguridad digital, SARLAFT y riesgos de corrupción estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información**

La Subred de servicios de salud norte, dentro del alcance de la POLÍTICA DE GESTIÓN Y ADMINISTRACIÓN DEL RIESGO, aprobada en el comité institucional de gestión y desempeño el día 22 de octubre de 2022, incluyó el compromiso en la gestión de los riesgos de seguridad digital definidos en el Modelos de Seguridad y privacidad de la información.

Roles y responsabilidades COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

7.1.5 Roles y responsabilidades

Como máxima autoridad del sistema de Gestión de riesgos de Seguridad y privacidad de la información esta el comité institucional de gestión y desempeño, a través de este, permitirá la aprobación de plan de tratamiento de riesgos, aprobación de la clasificación de los activos de información, aprobación del mapa de riesgos, aprobación del tratamiento del riesgo, notificaciones de la materialización del riesgo, entre otros.

7.5.5.1. Rol del Oficial de seguridad

La Subred de Servicios de Salud Norte ESE, con el fin de avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, realiza la contratación de un profesional en la modalidad de orden de prestación de servicios para el perfil de oficial de seguridad, quien será el responsable de la Seguridad de la Información, y las obligaciones que deberá cumplir respecto a la gestión del riesgo de seguridad están relacionados por los lineamientos emitidos por el MinTIC:

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 34 de 43
		FECHA: 31/12/2022

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Actuar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

Ilustración 6: Rol del Oficial de Seguridad

Fuente: Modelo nacional de gestión de riesgos de la seguridad de la información en la entidades públicas - MinTIC)

7.1.6 Identificación de Activos de información

En esta etapa se deben identificar los Activos de Información, para esta identificación se aplicará la guía para la gestión y clasificación activos de información establecida por MinTIC, la cual establece las directrices para la clasificación de los activos a los que se les debe brindar mayor protección.

Es importante tener en cuenta que es un activo de información: son recursos que poseen información y conocimiento importante sobre la organización.

En el contexto de seguridad de la información, se consideran activos de información:

- ✓ Aplicaciones de la organización
- ✓ Servicios web
- ✓ Redes
- ✓ Información física o digital
- ✓ Tecnologías de información TI
- ✓ Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

De acuerdo con lo anterior las actividades para realizar el inventario de activos son:

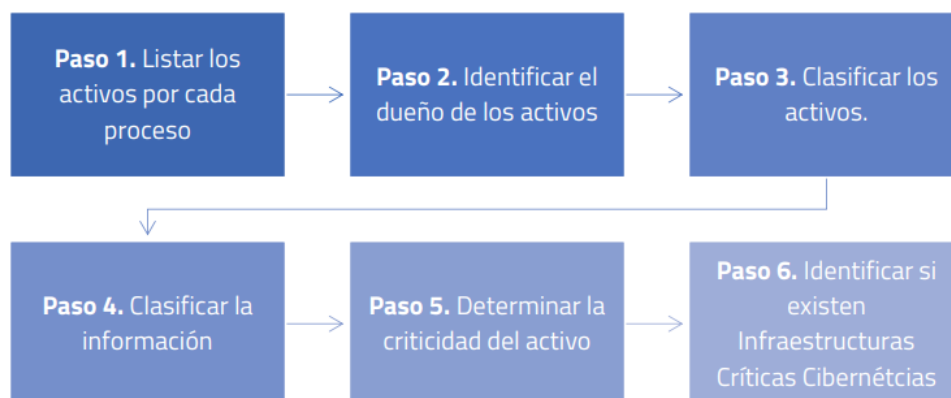


Ilustración 7: Pasos para identificar y Valorar los activos de información

Fuente: Modelo nacional de gestión de riesgos de la seguridad de la información en la entidades públicas - MinTIC)

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 35 de 43
		FECHA: 31/12/2022

A continuación, se detalla lo que deberá tenerse en cuenta para la realización de cada uno de los pasos mencionados para la identificación y valoración de activos de la información.

Paso 1. Listar los activos por cada proceso: cada proceso, deberán listar los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Paso 2. Identificar el dueño o propietario de los activos: Cada uno de los activos identificados deberá tener un dueño designado, si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Paso 3. Clasificar los activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza, ejemplo: Información, Software, Hardware, Componentes de Red entre otros. La siguiente tabla presenta la tipología de activos con el fin de hacer la clasificación mencionada.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Recurso Humano (Personas)	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa
Otros	Activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso

Ilustración 8: Tipología de Activos

Fuente: Modelo nacional de gestión de riesgos de la seguridad de la información en la entidades públicas - MinTIC)

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 36 de 43 FECHA: 31/12/2022

Paso 4. Clasificar la información: Se debe realizar la clasificación de la información conforme lo establecen las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos.

Paso 5. Determinar la criticidad del activo (Valoración del Activo): Evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno. Conforme lo establecido en la Metodología de Activos de Información se valoraron los activos respecto a la confidencialidad, integridad y disponibilidad mediante las escalas (ALTA-5, MEDIA-3 y BAJA-1) que identifican su nivel de importancia o criticidad para el proceso. La Entidad define gestionar los riesgos solo en aquellos que tengan un nivel de **criticidad Alto**, tomando como referencia la Guía de Gestión del Riesgo del MinTIC.

			CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD
MAYOR Y CATASTRÓFICO 100 Y 500 SMLV	Afecta la imagen con efecto publicitario sostenido	ALTO 5	Exposición información personal y sensible Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MENOR Y MODERADO 10 Y 100 SMLV	Afecta usuario de relevancia con el logro de objetivos y la imagen internamente	MEDIO 3	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
LEVE (Menor a 10 SMLV)	No afecta o afecta levemente algún área interna	BAJO 1	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

Tabla 17: Evaluar la criticidad de los activos de información
(Fuente: Guía para la Gestión y Clasificación de Activos de Información-Guía 5)

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 37 de 43 FECHA: 31/12/2022

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas - ICC: Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	\$464.619.736	3 años en recuperación

*Ilustración 9: Criterios Infraestructuras Críticas Cibernéticas –
Fuente: ICC (Comando Conjunto Cibernético (CCOC), Comando General Fuerzas*

7.1.7 Identificar los Riesgos

Como lo indica la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos y conjuntamente analizar las **posibles amenazas y vulnerabilidades** que podrían causar su materialización e identificar su consecuencia, es decir se identifica los daños o las consecuencias que podrían ser causadas por un incidente.

7.1.7.1 Describir el riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso, el DAFP propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos

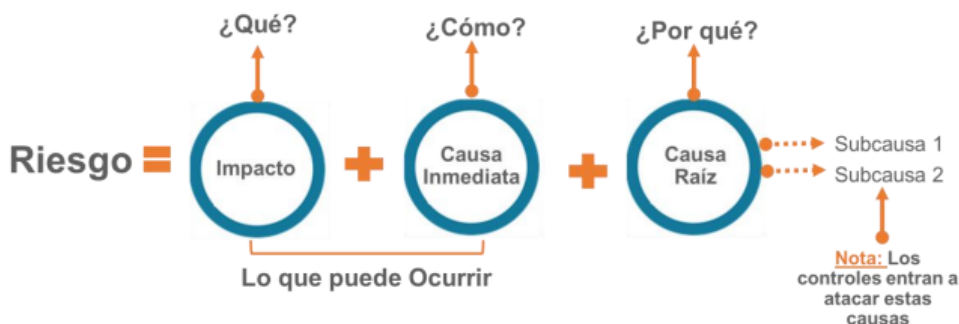


Ilustración 10: Estructura propuesta para la redacción del riesgo

(fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020)

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 38 de 43
		FECHA: 31/12/2022

7.1.8 Valorar los riesgos

Posterior a la identificación de los riesgos de seguridad digital con sus respectivas amenazas y vulnerabilidades, se deberá continuar con el Paso 3. Valoración del Riesgo, de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP.

Por medio de la estimación del riesgo, se busca establecer la probabilidad de ocurrencia del riesgo y su nivel de impacto, con el fin de estimar la zona de riesgo inicial, llamada riesgo inherente, y de esta forma realizar su priorización y establecer la estrategia de tratamiento.

Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Ilustración 11: Criterios para definir el nivel de probabilidad

Fuente:(Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Análisis de Impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo, entendiendo que el impacto es la consecuencia económica y reputacional que se genera por la materialización del riesgo.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 39 de 43
		FECHA: 31/12/2022

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Ilustración 12: Criterios para definir el nivel de impacto

Fuente:(Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Una vez se realice el análisis inicial (riesgo inherente), se procede a definir el nivel de severidad para el riesgo de seguridad de la información utilizando la matriz de claro establecida por el DAFP.

		Impacto				
Probabilidad	Muy Alta 100%					Extremo
	Alta 80%					Alto
	Media 60%					Moderado
	Baja 40%					Bajo
	Muy Baja 20%					
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Ilustración 13:Matriz de calor

Fuente:(Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.1.9 Identificación y evaluación de los controles existentes

De acuerdo con la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP, una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para mitigar/tratar los riesgos, para ello se utilizará el Anexo A de la Norma ISO/IEC 27001:2013 como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad de la información que están enunciados en dicho anexo y el manual de riesgos del DAF

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de DocumentosNo haga copias de este documento porque corre el riesgo de tener una versión desactualizada

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 40 de 43 FECHA: 31/12/2022

7.1.10 Definición y aprobación de mapas de riesgos y planes de tratamiento

Una vez terminada las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, los líderes de los procesos deberán emitir la aprobación de los mapas de riesgos, a través del Comité Institucional de Gestión y Desempeño. De igual forma aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos priorizados, cuyo nivel de riesgo inherente este en zona Moderada, Alta o Extrema.

7.1.11 Evaluación del Riesgo residual

Luego de definir y ejecutar las acciones del plan de tratamiento, se debe estimar el Riesgo Residual después de haber ejecutado las acciones, para esta actividad es necesario tener en cuenta la tabla de resultado de los posibles desplazamientos de probabilidad e impacto de la Guía para la Administración de los Riesgos de Gestión y Seguridad de la información y el Diseño de Controles en Entidades Públicas (DAFP y MinTIC).

Una vez identificados los riesgos residuales se pueden tomar acciones como:

Controlar el riesgo: Fortalecer o implementar nuevos controles

Eliminar el riesgo: Se elimina el activo y por consiguiente se elimina el riesgo

Compartir el riesgo: Mediante acuerdos se traspasa una parte o totalidad del riesgo a un tercero.

7.1.12 Plan de tratamiento de riesgos materializados

En el caso de materializarse un riesgo, este debe ser reportado inmediatamente en el Comité Institucional de Gestión y Desempeño y proceder a:

1. Ejecutar plan de contingencia.
2. Analizar el riesgo y validar en qué nivel queda posterior a la materialización
3. Registrar los cambios respectivos en el mapa de riesgos.
4. Realizar el análisis de causa y levantar plan de mejoramiento
5. En caso en que el riesgo que no esté identificado, este deberá ser reportado para que se inicie su correspondiente identificación en la matriz y se formule el plan de mejoramiento.
6. Informe detallado de la materialización de riesgo
7. Seguimiento y mejoramiento a los controles.

7.2 FASE DE EJECUCIÓN

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo de la fase de planeación.

7.3 FASE DE MONITOREO Y REVISIÓN

El responsable de seguridad de la información, deberá supervisar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes ejecuten las tareas en los tiempos pactados y que los

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 41 de 43
		FECHA: 31/12/2022

recursos se estén ejecutando de acuerdo con lo planeado.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública.

El monitoreo y seguimiento se reporta en el Comité Institucional de Gestión y Desempeño.

7.4 MEJORAMIENTO CONTINUO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION

La Entidad debe garantizar la mejora continua de la gestión de riesgos de seguridad y privacidad de la información, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos.

7.5 PLAN DE TRABAJO

Las actividades planteadas a continuación fortalecen la gestión de los riesgos de seguridad y privacidad de la Información Para la vigencia 2023 se planean adelantar las siguientes actividades por parte Gestión de Sistemas de Información – TIC y el equipo de seguridad de la Información:

ACTIVIDAD	ACCION	RESPONSABLE	FECHA INICIO	FECHA FINAL	INDICADOR
Procedimiento de levantamiento y actualización de activos de información.	Documentar el procedimiento de levantamiento y actualización de activos de información, estableciendo las directrices y actividades generales para identificar, clasificar y valorar los activos de información de la Subred	Grupos de seguridad de Seguridad de la información	1/01/2023	31/03/2023	% de avance de la documentación
Sensibilización sobre activos de información con el fin de identificar, clasificar y valorar los activos de información de la Subred.	Realizar socialización sobre el significado e importancia de los activos de información a todos los líderes de proceso.	Grupos de seguridad de Seguridad de la información	01/03/2023	30/04/2023	(No. de funcionarios y contratistas sensibilizados * proceso/Total de funcionarios y contratistas por proceso) * 100
Elaborar la matriz de activos de información de acuerdo con la Guía de MinTIC y al procedimiento documentado	Diseñar la estructura de la matriz de activos de información, de acuerdo con las variables sugeridas por MinTIC.	Grupos de seguridad de Seguridad de la información	01/04/2023	30/04/2023	% de avance en la elaboración de la matriz de activos de información
Levantamiento de activos de información.	Relación de activos de información por proceso	Líderes de proceso	01/05/2023	30/06/2023	(No. de activos caracterizados por proceso/Total de

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 42 de 43
		FECHA: 31/12/2022

					activos por proceso) *100
Identificar los riesgos de los activos de información de acuerdo con la metodología de gestión de riesgos de Seguridad de la Información del DAFP y MINTIC.	Descripción de los riesgos identificando los principios de seguridad de la información (Confidencialidad, integridad, disponibilidad)	Grupos de seguridad de Seguridad de la información	1/07/2023	30/09/2023	(Número de riesgos materializados/Total de Riesgos identificados) * 100
Análisis y evaluación de riesgos de seguridad	Realizar identificación, análisis y valoración de los riesgos (probabilidad e impacto)	Grupos de seguridad de Seguridad de la información	1/07/2023	30/09/2023	% de avances en la valoración de riesgos.
Definir los controles y formular el plan de tratamiento para el análisis y gestión de los activos de información de acuerdo con la metodología de gestión de riesgos del DAFP.	Definir Controles según análisis de riesgos Definir las actividades o acciones a realizar Elaborar plan de tratamiento de riesgos	Grupos de seguridad de Seguridad de la información	01/10/2023	31/10/2023	% de avance en la definición de controles
Definición y aprobación de mapas de riesgos y planes de tratamiento	Socializar plan de tratamiento de riesgos	Grupos de seguridad de Seguridad de la información	01/11/2023	30/11/2023	Plan de tratamiento de riesgos aprobado
Publicación de riesgos de seguridad de información	Realizar publicación del plan de tratamiento de riesgos aprobado.	Grupos de seguridad de Seguridad de la información	01/12/2023	31/12/2023	Publicación de Plan de tratamiento
Evaluación Riesgo residual	Estimar el Riesgo Residual después de haber ejecutado las acciones	Grupos de seguridad de Seguridad de la información	01/12/2023	31/12/2023	% de efectividad de los controles.
Implementación del Plan de tratamiento	Implementar los planes de tratamiento de riesgos definidos en la fase de planificación	Grupos de seguridad de Seguridad de la información	01/12/2023	31/12/2023	% de implementación del plan de tratamientos
Monitoreo y revisión del plan de tratamiento de riesgo	Generar y presentar informes de gestión de riesgos	Grupos de seguridad de Seguridad de la información	01/12/2023	31/12/2023	Informe de seguimiento del plan de tratamiento de riesgos de activos de información
Mejoramiento	Identificar oportunidades de mejora con los resultados obtenidos	Grupos de seguridad de Seguridad de la información	01/12/2023	31/12/2023	Planes de mejoramiento evaluados

Tabla 18: Plan de trabajo Gestión de Riesgo de seguridad y privacidad de la información

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-03-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTION TICS	Página 43 de 43
		FECHA: 31/12/2022

8. BIBLIOGRAFÍA

- Guía para la administración del Riesgo del Departamento Administrativo de la Función Pública – DAFP.
- CONPES 3701 de 2011 sobre los lineamientos de políticas para la ciberseguridad y ciberdefensa de la República de Colombia.
- Documento de Análisis y consulta de Identificación de posibles acciones regulatorias a implementar en materia de ciberseguridad, de la Comisión de Regulación de Comunicaciones – CRC de julio de 2015 de la República de Colombia.
- ISO 27005 de 2018
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en entidades pública - MinTIC

CONTROL DEL DOCUMENTO			
Versión	Fecha	Descripción de la modificación	Realizada por
1	08/08/2018	Creación	Nombre: Norberto Ruiz Rodríguez Cargo: Jefe Oficina Sistemas de Información - TIC
2	31/05/2019	Se agrega anexo de la priorización de los planes de Sistema Único de Acreditación	Nombre: Yolanda Ma. Cardozo Herrera. Cargo: Profesional Universitario
3	19/12/2022	Se adiciona la metodología de gestión de riesgo de seguridad y privacidad de la información y el plan de trabajo para el 2023	Nombre: Jeiffe Yubeli Muñoz Cargo: Oficial de Seguridad de la Información. Nombre: Edna Lizeth Villarreal Cargo: Profesional Especializado II

Elaboró:	Revisó:	Aval técnico de normalización:	Aprobó:
Nombre: Yolanda Bernal González	Nombre:	Nombre:	Nombre:
Cargo: Jefe Oficina Sistemas de Información – TIC (E)	Cargo:	Cargo:	Cargo:
ORIGINAL FIRMADO			