

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

TABLA DE CONTENIDO

INTRODUCCIÓN	3
1. OBJETIVO	3
1.1. OBJETIVOS ESPECIFICOS	4
2. ALCANCE	4
3. DEFINICIONES.....	5
4. MARCO LEGAL	7
5. RESPONSABILIDADES	9
6. TALENTO HUMANO REQUERIDO	10
7. MATERIALES, INSUMOS Y EQUIPOS REQUERIDOS	10
8. MARCO TEORICO.....	11
9. DESARROLLO.....	12
9.1 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	12
9.1.1 Objetivos de Seguridad y Privacidad de la Información	13
9.1.2 Compromiso de la Alta Dirección.....	13
9.2 CICLO DE OPERACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	14
9.3 FASE PREVIA DE DIAGNÓSTICO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	15
9.4 FASE DE PLANEACIÓN	17
9.4.1 Alcance del Plan de Seguridad y Privacidad de la Información.....	18
9.4.2 Gobierno de la Seguridad y Privacidad de la Información.....	18

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

9.5	FASE DE IMPLEMENTACIÓN	19
9.6	FASE DE EVALUACIÓN DEL DESEMPEÑO	22
9.6.1	Seguimiento y Medición.....	22
9.7	FASE DE MEJORA DEL SGSI	23
9.8	PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DEL MODELO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	25
9.9	PROCESO DE BUENAS PRÁCTICAS DE SEGURIDAD PARA MANEJO TRANSACCIONAL	29
9.9.1	Riesgos Originados por Incidentes de Delito Informático	29
9.9.2	Buenas prácticas de Entidades Públicas en el Componente de Tecnología Seguridad y Ciberseguridad de la Información:	30
9.9.3	Principales Riesgos Asociados a las Entidades Públicas	33
9.9.4	Buenas Prácticas de Entidades Públicas en el Componente de Seguridad de la Información para el Manejo de sus Productos Financieros	34
10.	SEGUIMIENTO Y EVALUACIÓN	36
11.	ANEXOS	37
12.	DOCUMENTOS RELACIONADOS	37
13.	BIBLIOGRAFIA	37

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

INTRODUCCIÓN

La información es el activo más importante y relevante para las organizaciones, así como aquellos que soportan y recurso indispensable para el desarrollo y cumplimiento misional junto con los compromisos del negocio; ésta puede llegar a ser sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesario para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

En atención a las situaciones de riesgo expuestas anteriormente, se genera entonces por parte de la gerencia de la Red de Salud del Centro ESE, la iniciativa de establecer, implementar y mantener un Plan de Seguridad y Privacidad de la Información enfocado en alcanzar y mantener una cultura y conciencia en el acceso y uso adecuado de la información en la institución. El presente documento identifica y recopila buenas prácticas para la gestión del ciclo de operación del Plan de Seguridad y Privacidad de la Información, a partir de una evaluación de diagnóstico, planeación, implementación, gestión y mejora continua del mismo.

1. OBJETIVO

Presentar el plan de seguridad y privacidad de la información de la Red de Salud del Centro ESE y los elementos que lo conforman, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

adecuado de la información y activos de información que la soportan al interior de la Institución para los años del 2024 al 2027.

1.1. OBJETIVOS ESPECIFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad, se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Orientar a los usuarios en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

2. ALCANCE

El presente documento identifica e incluye las orientaciones para la gestión del ciclo de operación del Plan de Seguridad y Privacidad de la Información, el cual debe ser aplicado sobre todos los procesos de la Red de Salud del Centro ESE y de cumplimiento por parte de todos los colaboradores.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

3. DEFINICIONES

Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

Amenaza Cibernética: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Incidentes de seguridad de la información: Eventos que comprometen la confidencialidad, integridad o disponibilidad de la información.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Políticas: Directrices u orientaciones por las cuales la alta dirección define el marco de actuación con el cual se orientará la actividad pública en un campo específico de su gestión, para el cumplimiento de los fines constitucionales y misionales de la entidad, de manera que se garantice la coherencia entre sus prácticas y sus propósitos.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Seguridad de la Información: Se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. (ISO27001).

SGSI (Sistema de Gestión de Seguridad de la Información): Es un conjunto de políticas, procedimientos, controles y recursos que permiten gestionar de manera sistemática la

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

seguridad de la información dentro de una organización. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de los datos, protegiéndolos frente a amenazas internas y externas, cumpliendo con la normativa aplicable y alineándose con los objetivos estratégicos. El SGSI se basa en estándares internacionales como ISO/IEC 27001, y se implementa mediante un enfoque de mejora continua (ciclo PDCA: Planificar, Hacer, Verificar, Actuar), que incluye: Identificación y análisis de riesgos relacionados con la información, Definición de controles y políticas para mitigar riesgos, Monitoreo y auditoría del desempeño del sistema, Acciones correctivas y preventivas para garantizar su evolución.

Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, como en el software.

4. MARCO LEGAL

La Política de Seguridad y Privacidad de la Información se fundamenta en el cumplimiento de la normativa nacional e internacional que regula la protección de datos personales, la gestión documental, la transparencia y la seguridad digital. Este marco incluye leyes, decretos y estándares como la Ley 1581 de 2012 sobre protección de datos, la Ley 1712 de 2014 sobre acceso a la información pública, los decretos reglamentarios asociados, así como la Norma ISO/IEC 27001:2022, que establece lineamientos para garantizar la confidencialidad, integridad

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

y disponibilidad de la información. Estas disposiciones orientan las acciones institucionales para proteger los activos de información y asegurar su uso responsable y seguro.

Norma	Descripción / Objeto
Norma ISO/IEC 27001:2022	Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
Ley 1952 de 2022	Código General Disciplinario
Ley 1915 de 2019	Modifica Ley 23 de 1982 sobre derecho de autor y derechos conexos
Ley 1712 de 2014	Ley de Transparencia y Derecho de Acceso a la Información Pública.
Ley 1581 de 2012	Disposiciones generales para la protección de datos personales.
Decreto 1263 de 2022	Lineamientos y estándares aplicables a la Transformación Digital Pública.
Decreto 767 de 2022	Lineamientos generales de la Política de Gobierno Digital.
Decreto 338 de 2022	Adiciona Título 21 al Decreto 1078 sobre TIC.
Decreto 620 de 2020	Reglamenta uso y operación de servicios ciudadanos digitales.
Decreto 2106 de 2019	Estrategia de seguridad digital en trámites y procesos digitales.
Decreto 1008 de 2018	Lineamientos generales de la política de Gobierno Digital.
Decreto 612 de 2018	Directrices para integración de planes institucionales y estratégicos.
Decreto 1499 de 2017	Modifica Decreto 1083 sobre Sistema de Gestión.
Decreto 728 de 2017	Fortalecimiento del modelo de Gobierno Digital.
Decreto 1083 de 2015	Políticas de Gestión y Desempeño Institucional (Gobierno Digital y Seguridad Digital).
Decreto 1080 / 1081 de 2015	Reglamentación sectores Cultura y Presidencia.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC.
Decreto 1074 de 2015	Reglamenta Ley 1581 y Registro Nacional de Bases de Datos.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

Norma	Descripción / Objeto
Decreto 103 de 2015	Reglamenta parcialmente Ley 1712.
Decreto 886 de 2014	Reglamenta Registro Nacional de Bases de Datos.
Decreto 1377 de 2013	Reglamenta parcialmente Ley 1581.
Decreto 2609 de 2012	Reglamenta Ley 594 y Ley 1437 sobre Gestión Documental.
CONPES 4144 de 2025	Política Nacional de Inteligencia Artificial.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.
CONPES 3975 de 2019	Política Nacional para la Transformación Digital e Inteligencia Artificial.

5. RESPONSABILIDADES

Rol	Responsabilidad
Gerencia	Aprobar el Plan de Seguridad y Privacidad de la Información.
Subgerencias	Aprobar el Plan y garantizar su alineación con las directrices estratégicas.
Líder del proceso de gestión de tecnologías y la información	Socializar el plan con las áreas involucradas y promover su correcta implementación.
Líderes	Desarrollar el plan y asegurar la implementación de controles y procedimientos definidos.
Colaborador de cada proceso	Ejecutar y desarrollar el plan en sus áreas, cumpliendo las políticas y protocolos establecidos.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

6. TALENTO HUMANO REQUERIDO

Cargo / Perfil	Responsabilidad	Competencia requerida
Ingeniero Industrial	Implementar el SGSI (Sistema de Gestión de Seguridad de la Información) en todos los procesos organizacionales.	• Conocimiento en normas ISO/IEC 27001 • Gestión de riesgos y procesos • Habilidades en planificación y liderazgo • Capacidad para elaborar políticas y procedimientos.
Técnico de Sistemas	Apoyar la implementación del SGSI en la parte digital, asegurando la correcta configuración y seguridad tecnológica.	• Conocimiento en ciberseguridad y redes • Manejo de sistemas operativos y servidores • Familiaridad con herramientas de monitoreo y control • Capacidad para aplicar protocolos de seguridad digital.
Técnico de Gestión Documental	Apoyar la implementación del SGSI en la parte física, garantizando la adecuada gestión y protección de documentos.	• Conocimiento en gestión documental y normativas archivísticas. • Manejo de sistemas de información documental. • Habilidades en organización y custodia de archivos. • Capacidad para aplicar políticas de seguridad física.

7. MATERIALES, INSUMOS Y EQUIPOS REQUERIDOS

Para garantizar la correcta implementación de la Política de Seguridad y Privacidad de la Información, es necesario contar con materiales, insumos y equipos que respalden las acciones definidas en el plan.

Estos recursos permiten establecer controles efectivos, asegurar la protección de los activos de información y facilitar la capacitación y sensibilización del personal, contribuyendo al cumplimiento normativo y a la mitigación de riesgos, tales como:

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

- Herramientas para cifrado y protección de datos.
- Licencias de antivirus y sistemas de protección perimetral.
- Material didáctico para capacitaciones (presentaciones, guías, videos).
- Recursos para campañas de sensibilización (afiches, boletines, correos).
- Servidores seguros para almacenamiento de información.
- Equipos de cómputo con configuraciones de seguridad actualizadas.
- Dispositivos de respaldo (discos duros externos, sistemas de backup).
- Equipos de red (routers, firewalls, switches) con protocolos de seguridad.
- Sistemas biométricos o de control de acceso físico.

8. MARCO TEORICO

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un estado más participativo, más eficiente y transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

9. DESARROLLO

9.1 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad de información es la declaración general que representa la posición de la RED DE SALUD DEL CENTRO ESE frente a la necesidad de protección de su información, al igual que de la preservación de aquellos activos de información que la soportan, por tal motivo define que:

“La RED DE SALUD DEL CENTRO ESE reconoce el valor de su información como uno de sus activos más valiosos y es consciente de la necesidad de su custodia, conservación, disponibilidad, integridad, accesibilidad y confidencialidad en los casos que corresponda, generando una cultura de protección y uso adecuado a través de la implementación y mejora continua de un sistema de gestión de seguridad de la información, con un enfoque de administración y tratamiento de riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales, que permitan asegurar la confianza de las partes interesadas”.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

9.1.1 Objetivos de Seguridad y Privacidad de la Información

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la RED DE SALUD DEL CENTRO ESE, se declaran los siguientes objetivos generales:

- Establecer las directrices y lineamientos relativos a seguridad de la información.
- Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos.
- Implementar mecanismos de control para la protección de los datos, la información y los recursos asociados que los soportan.
- Asegurar que los riesgos asociados a seguridad de la información se mantienen en un nivel aceptable.
- Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

9.1.2 Compromiso de la Alta Dirección

La gerencia de la RED DE SALUD DEL CENTRO ESE aprueba la política general de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento y mejora continua de políticas y lineamientos consecuentemente orientados a la salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Institución.

- Su compromiso se demostrará a través de:
- La revisión y aprobación de políticas y lineamientos de seguridad de la información.
- La promoción de una cultura de seguridad y protección de la información.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: GTI-PO-005		
	Fecha de entrada en vigencia: 19/01/2026		
	Versión 04		

- El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a los servidores públicos y partes interesadas.
- La asignación de los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- La realización de actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

9.2 CICLO DE OPERACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la etapa inicial de los propósitos de diseño del sistema de gestión de seguridad de la información, se identificó la necesidad de definir las 5 fases que orientarían el ejercicio para los propósitos de protección de la información de la Institución bajo un modelo sostenible: previa de diagnóstico, planeación, implementación, evaluación del desempeño y fase de mejora.

Ilustración 1. Esquema del Modelo del Sistema de Gestión de Seguridad de la información



Fuente: Elaboración propia

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

9.3 FASE PREVIA DE DIAGNÓSTICO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimiento de requisitos y lineamientos de seguridad de la información, y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Institución.

El resultado de la evaluación diagnóstica permite determinar el nivel de madurez del ciclo operativo del Plan de Seguridad y Privacidad de la Información en la RED DE SALUD DEL CENTRO ESE, así como definir el mapa de ruta para las actividades clave correspondientes a las fases de diseño y establecimiento del modelo.

Dichos hallazgos constituyen el insumo principal para iniciar la fase de planeación de cada uno de los ítems evaluados, en el marco del desarrollo de la herramienta de autodiagnóstico de seguridad y privacidad de la información diseñada para la Red de Salud del Centro ESE. Ver

Ilustración 2

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

Ilustración 2. Herramienta de autodiagnóstico de seguridad y privacidad de la información de la Red de Salud del Centro ESE

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	18	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	72	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	52	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	61	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	45	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	41	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	100	REPETIBLE
A.18	CUMPLIMIENTO	22.5	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		34	100	REPETIBLE

Fuente. Herramienta de autodiagnóstico de seguridad y privacidad de la información de la Red de Salud del Centro ESE

9.3.1 Herramienta de autodiagnóstico de seguridad y privacidad de la información

La herramienta de autodiagnóstico de seguridad y privacidad de la información para la Red de Salud del Centro ESE es un instrumento metodológico diseñado para evaluar el nivel de madurez y efectividad de los controles implementados en distintos dominios de la gestión de seguridad de la información. Su propósito principal es ofrecer una visión estructurada y objetiva del estado actual del modelo, identificar brechas frente a los niveles deseados, y orientar la planificación estratégica para su fortalecimiento.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

Características generales:

- **Enfoque por Dominios:** Evalúa áreas clave como políticas, gestión de activos, control de acceso, criptografía, continuidad del negocio, entre otros, alineados con estándares internacionales de seguridad de la información.
- **Calificación cuantitativa y cualitativa:** Cada dominio recibe una puntuación actual y una meta, complementadas con una clasificación del nivel de efectividad del control (por ejemplo, "Inicial", "Repetible", "Gestionado", "Efectivo", "Inexistente").
- **Diagnóstico integral:** Permite visualizar el promedio general de madurez de los controles, facilitando la toma de decisiones informadas para la mejora continua del modelo.
- **Base para la planeación:** Los resultados obtenidos sirven como insumo para definir el mapa de ruta de las fases de diseño, establecimiento y fortalecimiento del Plan de Seguridad y Privacidad de la Información.
- **Adaptabilidad Institucional:** Está contextualizada para el entorno de la Red de Salud del Centro ESE, lo que garantiza su pertinencia y aplicabilidad en el marco de la función pública.

9.4 FASE DE PLANEACIÓN

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto de la RED DE SALUD DEL CENTRO ESE, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

la información, entre ellos, la justificación, el alcance, la política y los objetivos del Plan de Seguridad y Privacidad de la Información.

9.4.1 Alcance del Plan de Seguridad y Privacidad de la Información

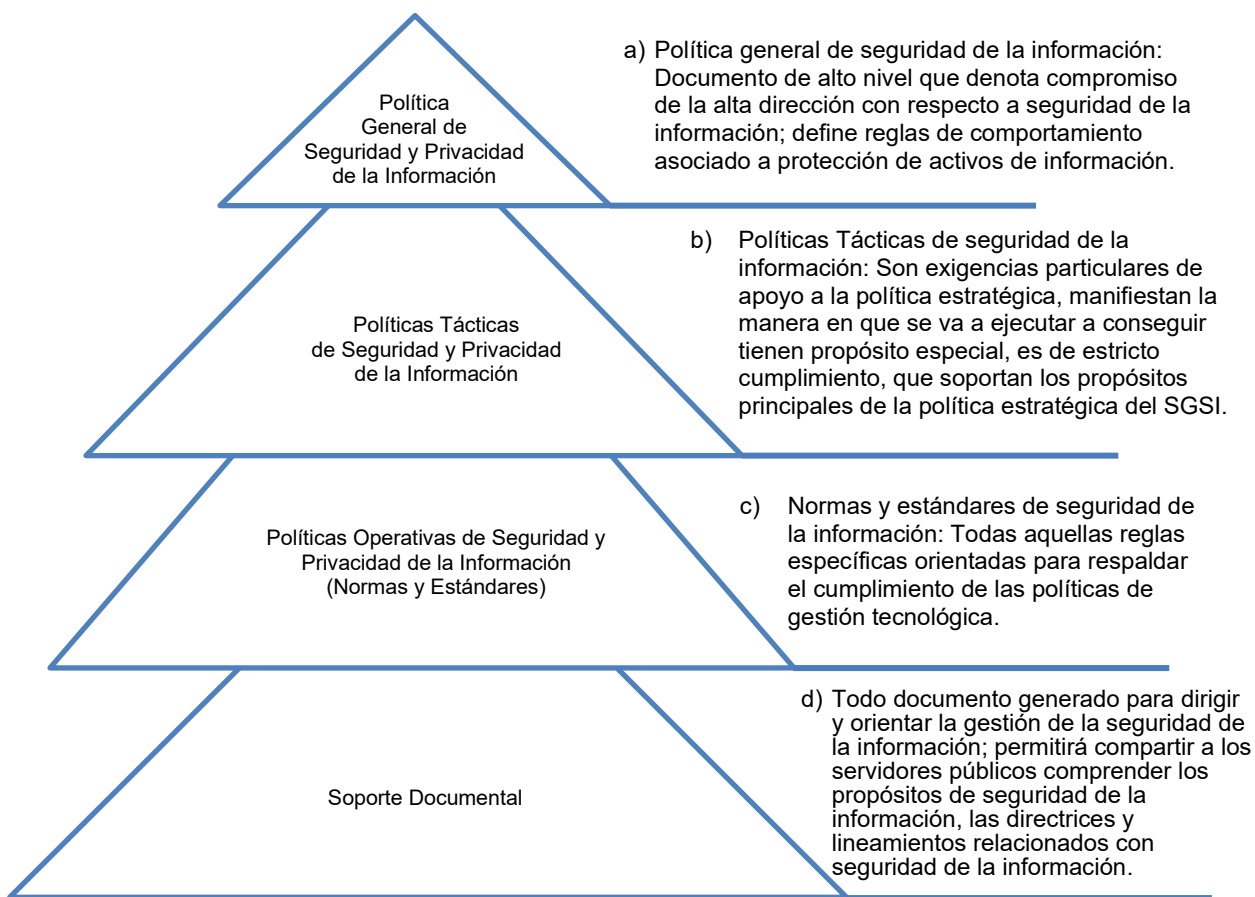
El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la gerencia de la RED DE SALUD DEL CENTRO ESE, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la institución y, de cumplimiento por parte de todos aquellos colaboradores y terceros que presten sus servicios o tengan algún tipo de relación con la Institución.

El alcance del plan de seguridad y privacidad de la información permitirá a la RED DE SALUD DEL CENTRO ESE definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del plan de seguridad y privacidad de la información con otros procesos.

9.4.2 Gobierno de la Seguridad y Privacidad de la Información

El modelo de gobierno de la seguridad de la información se presentará a través de una estructura de directrices y lineamientos por niveles de acuerdo con el propósito de cada uno de ellos. [Ilustración 3](#). La estructura de directrices y lineamientos de seguridad de la información se define de la siguiente manera:

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	



Fuente: Elaboración Propia

Toda la documentación asociada al sistema de gestión de seguridad de la información deberá ser revisada y actualizada (en la medida que aplique) bajo un estricto control de cambios para asegurar la integridad de los contenidos.

9.5 FASE DE IMPLEMENTACIÓN

El Plan de Seguridad y Privacidad de la Información permitirá a la RED DE SALUD DEL CENTRO ESE llevar a cabo la implementación de los aspectos y requisitos presentados tanto

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

por el Plan de Seguridad y Privacidad de la Información, como los presentados por la norma ISO/IEC 27001:2013; de igual manera, la implementación de los controles de seguridad de la información, que por normativa o por resultado de la valoración de riesgos deban ser implementados.

El plan de control operacional establecerá las actividades y la programación para la implementación tanto de los requisitos, controles y buenas prácticas de seguridad y privacidad de la información en la RED DE SALUD DEL CENTRO ESE.

Como estrategia interna para la orientación de los propósitos de seguridad y privacidad de la información, se definen e implementan políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

Tabla 1. Actividades para la Implementación del Plan de Seguridad y Privacidad de la Información

Actividad	Descripción	Evidencia de Actividad
Realizar reconocimiento del contexto de la RED DE SALUD DEL CENTRO ESE (cuestiones internas y externas) con propósito de orientar el SGSI como apoyo a la estrategia gerencial.	Definir los escenarios para los cuales el Plan de Seguridad y Privacidad de la Información será soporte a la estrategia definida por la Gerencia de la RED DE SALUD DEL CENTRO ESE.	Documento con la identificación de las cuestiones internas y externas de la RED DE SALUD DEL CENTRO ESE
Reconocer las partes interesadas de la RED DE SALUD DEL CENTRO ESE e identificar sus necesidades y expectativas con respecto a seguridad de la información	Reconocer las necesidades y expectativas de seguridad de la información por cada una de las partes interesadas de la RED DE SALUD DEL CENTRO ESE, que permitan orientar esfuerzos de cumplimiento para cada una de ellas.	Documento con la identificación de las partes interesadas, sus necesidades y expectativas pertinentes a la seguridad de información

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

Actividad	Descripción	Evidencia de Actividad
Definir el alcance, políticas y objetivos del plan de seguridad y privacidad de la información.	Definir el alcance y los límites bajo los servicios, procesos o actividades propias de la RED DE SALUD DEL CENTRO ESE sobre el cual se implementará el Plan de Seguridad y Privacidad de la Información.	Documento con la identificación del alcance y límites, política y objetivos del plan de seguridad y privacidad de la información
Definir la estructura de roles y responsabilidades para la gestión de los propósitos del plan de seguridad y privacidad de la información y de las fases definidas	Definir y asignar formalmente la autoridad, roles y responsabilidades para la gestión y propósitos del modelo de seguridad y privacidad de información.	Documento con la identificación y asignación de roles y responsabilidades
Realizar la valoración y tratamiento de los riesgos de seguridad de la información.	Definir la estrategia para identificar, estimar, evaluar y tratar los riesgos asociados a la seguridad de la información en la RED DE SALUD DEL CENTRO ESE.	Metodología para la valoración y tratamiento de los riesgos de seguridad de la información
Definir el modelo y esquema de gestión de políticas y directrices de seguridad de la información.	Documentar el esquema de políticas y lineamientos de seguridad de la información en apoyo al cumplimiento de la política general de seguridad de la información de la RED DE SALUD DEL CENTRO ESE.	Manual de políticas y lineamientos de seguridad de la información
Ejecutar el plan de valoración y tratamiento de los riesgos de seguridad de la información	A través de la identificación del inventario de activos de información por procesos, identificar los riesgos de seguridad de la información asociados a los mismos y aplicar la mejor estrategia de tratamiento con propósito de obtener niveles de riesgo residuales aceptables.	Inventario de activos de información Mapa de riesgos de seguridad de la información
Realizar actividades de sensibilización y toma de conciencia de seguridad y privacidad de la información	Ejecución de plan de sensibilización y toma de conciencia de aspectos de seguridad de la información.	Plan de comunicación y resultados de actividades de seguimiento al cumplimiento
Definir e implementar los controles de seguridad de la información	Implementar las estrategias de mitigación de riesgos de seguridad de la información de acuerdo con resultado de valoración de riesgos y a los requisitos del Plan de Seguridad y Privacidad de la Información.	Plan de tratamiento de riesgos

Fuente: Elaboración propia

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

9.6 FASE DE EVALUACIÓN DEL DESEMPEÑO

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

9.6.1 Seguimiento y Medición

Para las actividades de seguimiento y medición, la RED DE SALUD DEL CENTRO ESE definirá procedimientos que permitan:

- Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Institución.
- Empezar revisiones regulares de la eficacia del plan de seguridad y privacidad de la información (que incluyen el cumplir de la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

- Realizar ejercicios de auditoría interna del plan de seguridad y privacidad de la información.
- Realizar actividades de revisión del plan de seguridad y privacidad de la información por parte de la gerencia de la RED DE SALUD DEL CENTRO ESE.

Tabla 2. Actividades para la Evaluación del Plan de Seguridad y Privacidad de la Información

Actividad	Descripción	Evidencia de Actividad
Definir y ejecutar el plan de evaluación de desempeño del Plan de Seguridad y Privacidad de la Información.	La estrategia de evaluación de desempeño establecerá el alcance y escenarios sobre los cuales se realizará seguimientos y mediciones (ejemplo, requisitos de seguridad, estados de valoración de riesgos, implementación de planes de tratamiento, etc.), los métodos elegidos, la frecuencia y los responsables de su ejecución.	Documento con la identificación de la estrategia de evaluación de desempeño y criterios (seguimiento, medición, análisis y evaluación)
Definir y aprobar el programa de auditoría interna del Plan de Seguridad y Privacidad de la Información.	El programa de auditoría identificará la(s) auditoría(s) que serán realizadas para evaluar el Plan de Seguridad y Privacidad de la Información, al igual que el cronograma para su ejecución.	Documento con la identificación del programa de auditoría
Realizar la revisión del estado del Plan de Seguridad y Privacidad de la Información por parte de la alta dirección.	Recolectar las fuentes de información de aspectos del estado de operación del Plan de Seguridad y Privacidad de la Información para presentarlas ante la alta dirección.	Plan de revisión por la dirección Informe de resultados de la revisión por la dirección.

Fuente: Elaboración propia

9.7 FASE DE MEJORA DEL SGSI

La Institución con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tomará en cuenta los resultados de la fase III “Evaluación de desempeño” la cual está basada en los resultados de las actividades de seguimiento y medición (indicadores).

La RED DE SALUD DEL CENTRO ESE:

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

- Implementará las mejoras identificadas en el plan de seguridad y privacidad de la información
- Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.
- Implementará acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras compañías.
- Asegurar que las mejoras cumplen con los objetivos y propósitos definidos por la RED DE SALUD DEL CENTRO ESE.

Tabla 3. Actividades para la Mejora del Sistema de Seguridad y Privacidad de la Información

Actividad	Descripción	Evidencia de Actividad
Identificar, definir y activar planes de mejoramiento del plan de seguridad y privacidad de la información	Los resultados y conclusiones de las actividades de evaluación de desempeño del plan de seguridad y privacidad de la información permitirán identificar los escenarios sobre los cuales se podrán adoptar acciones correctivas o mejoras.	Plan de mejoramiento del plan de seguridad y privacidad de la información

Fuente: Elaboración propia

De acuerdo con la realización del autodiagnóstico de privacidad y seguridad de la información se muestra el avance de las etapas de planificación, implementación, evaluación de desempeño y mejora continua.

Componente	% Avance Actual Entidad	% Avance Esperado
Planificación	12%	40%
Implementación	5%	20%
Evaluación de Desempeño	4%	20%
Mejora Continua	4%	20%
Total	24%	100%

Fuente. Herramienta de autodiagnóstico de seguridad y privacidad de la información de la Red de Salud del Centro ESE

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

9.8 PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DEL MODELO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

9.8.1 SEGURIDAD

			2025		2026		2027	
	FASE	ACTIVIDAD	1 sem	2 sem	1 sem	2 sem	1 sem	2 sem
SEGURIDAD	Diagnostico	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.						
		Determinar el nivel de madurez de los controles de seguridad de la información.						
		Identificar el avance de la implementación del ciclo de operación al interior de la entidad.						
		Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.						
		Identificación del uso de buenas prácticas en ciberseguridad.						
	Planificación	Política de Seguridad y Privacidad de la Información						
		Procedimientos de seguridad de la información.						
		Roles y responsabilidades de seguridad y privacidad de la información.						
		Inventario de activos de información.						
		Integración del MSPI con el Sistema de Gestión documental						
		Identificación, Valoración y tratamiento de riesgo.						
		Plan de comunicaciones						
		Plan de diagnóstico de IPv4 a IPv6						

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

			2025		2026		2027	
	FASE	ACTIVIDAD	1 sem	2 sem	1 sem	2 sem	1 sem	2 sem
	Implementación	Planificación y Control Operacional.						
		Implementación del plan de tratamiento de riesgos.						
		Indicadores De Gestión.						
		Plan de Transición de IPv4 a IPv6						
	Evaluación y Desempeño	Plan de revisión y seguimiento, a la implementación del MSPI.						
		Plan de Ejecución de Auditorias						
	Mejora Continua	Plan de Mejora Continua						

Fuente. Elaboración propia

9.8.2 PRIVACIDAD

			2025		2026		2027	
	Fase	Actividad	1 sem	2 sem	1 sem	2 sem	1 sem	2 sem
PRIVACIDAD	Diagnostico	Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad.						
	Planificación	Documento con la política de privacidad, debidamente aprobada por la alta dirección y socializada al interior de la entidad.						
		Manual de políticas de seguridad y privacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad.						
		Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad.						
		Definición de roles en relación con la Información.						

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

		2025		2026		2027	
Fase	Actividad	1 sem	2 sem	1 sem	2 sem	1 sem	2 sem
	Procedimientos de privacidad.						
	Plan de capacitación al interior de la entidad						
	Implementación	Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información					
		Documento que evidencie el registro de las Bases de datos,					
		Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados					
	Evaluación y Desempeño	Documento con los resultados del plan de seguimiento					
		Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces					
		Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.					
	Mejora continua	Documento con los resultados del plan de seguimiento					
		Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces.					
		Documento con el consolidado de las auditorías.					

Fuente. Elaboración propia

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

9.8.3 ADOPCIÓN DEL PROTOCOLO IPV6

			2025		2026		2027	
	Fase	Actividad	1 sem	2 sem	1 sem	2 sem	1 sem	2 sem
ADOPCIÓN DEL PROTOCOLO IPV6	Planeación	Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada						
		Informe de la Infraestructura de red de comunicaciones						
		Recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de ipv6,						
		Plan de direccionamiento en ipv6						
		Plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con ipv6,						
		Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones						
		Documento que define la estrategia de para la implementación y aseguramiento del protocolo ipv6 en concordancia con la política de seguridad de las entidades.						
	Implementación	Documento con el informe de la implementación del plan y la estrategia de transición de ipv4 a ipv6, revisado y aprobado por la alta Dirección						
	Pruebas de Funcionalidad	Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación.						

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

			2025		2026		2027	
	Fase	Actividad	1 sem	2 sem	1 sem	2 sem	1 sem	2 sem
		Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación						
		Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo ipv6.						

Fuente. Elaboración propia

9.9 PROCESO DE BUENAS PRÁCTICAS DE SEGURIDAD PARA MANEJO TRANSACCIONAL

9.9.1 Riesgos Originados por Incidentes de Delito Informático

Los riesgos originados por incidentes de delito informático pueden ser variados y tienen el potencial de afectar a las entidades públicas. Es por esto tan importante conocerlos e implementar medidas de seguridad robustas, educando al personal sobre prácticas de seguridad y estableciendo prácticas regulares de seguridad, para mitigar estos riesgos.

A continuación, una descripción de las principales modalidades de delito informático identificados:

- Fraude electrónico:** Es la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, donde se influya en el procesamiento o el resultado de los datos de un

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema. (Referencia Código Penal, Ley N° 1273 de 2009).

2. **Phishing:** Fraude tradicionalmente cometido a través de internet, que pretende conseguir datos confidenciales de usuarios, tales como identificación o claves de acceso a cuentas de diversos sistemas. Una variante del Phishing, pero por teléfono se conoce como Vishing.
3. **Pharming:** Modalidad de estafa online (en línea) mediante la manipulación de los servidores DNS (Domine Name Server) para re-direccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales de usuarios como identificación o claves de acceso a cuentas de diversos sistemas.
4. **Phreaking:** Hacking orientado a la telefonía y estrechamente vinculado con la electrónica aplicada a los sistemas telefónicos.
5. **Humanware:** El factor humano que interviene en un sistema. Se refiere a las personas involucradas como usuarios, desarrolladores de aplicaciones, administradores, operadores, entre otros.

9.9.2 Buenas prácticas de Entidades Públicas en el Componente de Tecnología

Seguridad y Ciberseguridad de la Información:

Con el fin de mitigar la exposición a los riesgos derivados de las modalidades de delito informático mencionados, presentamos un compendio de buenas prácticas para Entidades Públicas.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

1. La seguridad de la información debe acompañarse de medidas complementarias, tanto en seguridad física como en estandarización de procesos, siguiendo un modelo de tipificación de los riesgos, asociado al modelo de madurez en seguridad de la información.
2. Implementar seguridad lógica y física en los equipos donde se realizan los giros de tesorería.
3. Protección física de la CPU de pagos y de su cableado para evitar cualquier manipulación de Hardware.
4. Licenciamiento del sistema operativo con estándares de seguridad.
5. Des-habilitación de puertos USB y unidades de CD/DVD.
6. IP fija registrada en el portal bancario, lo cual no permite realizar transacciones desde otro lugar.
7. Políticas de seguridad Active Directory desde el servidor principal.
8. Restricciones de Páginas de Correo, Redes Sociales, Generación de Historial de navegación, Archivos Temporales en los puntos de acceso a los portales bancarios.
9. Acceso a portales bancarios restringidos a los horarios semanales laborales. Lunes a Viernes de 8:00 am a 6:00 pm.
10. Cifrado de Archivos del sistema para impedir que terceros los puedan visualizar por fuera de la maquina principal.
11. Autenticación del usuario vía contraseña de Windows y su posterior Login al dominio del portal bancario con usuario y contraseña respectivos (token).
12. Empleo de herramientas de antivirus, antimalware, entre otras que identifiquen comportamientos inusuales en el equipo.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

13. Conexiones VPN seguras para transferencia de archivos y ordenes de transacciones de cara a los portales bancarios.
14. Cambios dinámicos y periódicos de contraseñas seguras.
15. Controles de acceso de celulares a las áreas de Tesorería.
16. Sistemas de monitoreo y grabación de las zonas transaccionales.
17. Implementación de políticas, procesos y procedimientos para estandarizar la gestión de la tesorería.
18. La estandarización de los canales transaccionales, a través de soluciones bancarias que cumplan con los lineamientos legales y garanticen la trazabilidad de la información y el manejo seguro de los recursos públicos.
19. La implementación de procesos que permiten el manejo adecuado de la información pública en lo relacionado con el cumplimiento de los protocolos de integridad y reserva de datos y las políticas de Habeas Data.
20. Hacer uso del portal transaccional, ingresando directamente a la página web dispuesta por la entidad, digitando completamente la dirección dentro del navegador y no mediante enlaces o accesos directos.
21. Hacer uso de la aplicación móvil que se encuentra registrada y disponible desde las tiendas oficiales, y no mediante archivos de instalación no autorizados.
22. No compartir sus credenciales y tokens, e implementar la configuración de contraseñas seguras.
23. Mantener actualizado el sistema operativo, el antivirus y las aplicaciones instaladas en los equipos.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

24. Se recomienda no habilitar bluetooth y conexiones Wi-Fi en lugares desconocidos para realizar transacciones o consultas.
25. Evitar hacer descargas de enlaces compartidos y desconocidos.
26. Mostrar enmascarados los productos de los clientes como cuentas de ahorros, cuentas corrientes, tarjetas débito, tarjetas crédito y créditos.
27. Establecer campañas de sensibilización a los usuarios sobre el uso de la tecnología, protección al consumidor, buenas prácticas de seguridad y prevención de fraude.

9.9.3 Principales Riesgos Asociados a las Entidades Públicas

Adicional a los incidentes de delito informático, las entidades públicas están expuestas a diferentes eventos de riesgo. Es importante que se implementen medidas de seguridad sólidas, que permitan la elaboración de evaluaciones de riesgos periódicas y el establecimiento de planes de respuesta a incidentes para mitigar estos riesgos y protejan los recursos públicos, la información sensible y los servicios esenciales que proporcionan a los ciudadanos.

A continuación, una descripción de los principales riesgos:

- 1. Fraude Interno:** Se refiere a actividades fraudulentas o engañosas realizadas por personas dentro de la entidad, ya sea de manera actual o pasada. Este tipo de fraude puede involucrar a empleados, gerentes o incluso a personas en posiciones de liderazgo y confianza dentro de la entidad.
- 2. Riesgo Legal:** Se refiere a la posibilidad de que la entidad o sus empleados se enfrenten a consecuencias negativas como resultado de acciones legales, incumplimientos de leyes, regulaciones o disputas legales. Este tipo de riesgo puede surgir de diversas áreas y

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

situaciones, y su impacto puede variar desde multas financieras hasta daños en la reputación o incluso implicaciones penales para las personas o las entidades.

3. **Fraude externo:** Se refiere a actividades fraudulentas o engañosas llevadas a cabo por individuos o entidades externas a la entidad (individuos, grupos organizados o incluso otras entidades o empresas).
4. **Fallas tecnológicas:** Se genera por fallos en los sistemas de cómputo, en el hardware o en el software de la entidad.
5. **Ejecución y gestión de procesos:** Se refiere a la posibilidad de que los procedimientos y actividades administrativas no se lleven a cabo de manera
6. eficiente, efectiva o conforme a las normativas establecidas. Típicamente se genera por un incorrecto procesamiento de las transacciones, o por un deficiente monitoreo y gestión de los presupuestos públicos.

9.9.4 Buenas Prácticas de Entidades Públicas en el Componente de Seguridad de la Información para el Manejo de sus Productos Financieros

1. Implementar procedimientos internos para los trámites de apertura, cancelación y/o cambio de firmas de cuentas bancarias necesarias para el manejo de los recursos propios y especiales, con el fin de mantener el adecuado registro, control y conciliación de las cuentas en los tiempos establecidos legalmente.
2. Implementar procedimientos internos para apertura y custodia de Títulos Valores con Entidades Financieras.
3. Implementar procedimientos internos para la custodia de chequeras de las cuentas corrientes dadas por las Entidades Financieras.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

4. Utilizar canales electrónicos autorizados para efectuar los pagos a los beneficiarios finales (Contratistas, Proveedores y funcionarios de la entidad por concepto de salarios y prestaciones sociales, descuentos de las nóminas, embargos judiciales, impuestos, servicios públicos y transferencias, Aportes de Salud y Pensión, entre otros, donde se le brinda el pago directo a la cuenta bancaria previamente definida y autorizada).
5. Utilizar medios y canales electrónicos para la reducción de los costos de manejo del efectivo y de chequeras (ahorro de tiempo y mayor seguridad), mejorando la transparencia en las transacciones y el control de los flujos de fondos.
6. Implementar un sistema de administración de cuentas corrientes y cuentas de ahorro, discriminadas por cada uno de los conceptos que se tienen (recursos de libre destinación, recursos de destinación específica, recursos especiales, recursos del crédito, recursos de dividendos).
7. Implementar las medidas de control y seguridad internos con el fin de garantizar el acceso a los canales transaccionales, emisión de órdenes de pago, traslados y demás operaciones bancarias, únicamente al funcionario facultado por los manuales de funciones internos de la Entidad.
8. Implementar estándares de calidad, seguridad e idoneidad para la contratación de terceros encargados de la revisión y mantenimiento de equipos e instalación de software o hardware que soportan la transaccionalidad con las entidades financieras.
9. Definir las competencias, roles y responsabilidades mínimos que debe cumplir el funcionario público designado por la entidad para el manejo de las transacciones, por los diferentes canales dispuestos por la Entidad Financiera.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
			Código: GTI-PO-005
			Fecha de entrada en vigencia: 19/01/2026
		Versión 04	

10. Garantizar que la totalidad de los pagos que realicen las entidades públicas se realicen con pago a cuenta.
11. Sobre los procesos de apertura de cuentas, actualización de información y de nuevos administradores, se debe crear una capa de control en las plataformas de Tecnologías de Información TI, para que el intercambio de información se realice garantizando los principios de seguridad de la información.
12. Adoptar protocolos que mitiguen el lavado de activos, en línea con las políticas de SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y Financiación al Terrorismo).
13. Adoptar protocolos para la mitigación de riesgos relacionados con malas prácticas como sobornos y condicionamientos contractuales (ABAC).

10. SEGUIMIENTO Y EVALUACIÓN

Nombre del Indicador	Objetivo
Oportunidad en el tratamiento de eventos o incidentes de seguridad relacionados en marco de seguridad y privacidad de la información = (Número de eventos o incidentes cerrados dentro del tiempo objetivo / Número total de eventos o incidentes reportados o detectados) * 100	Medir la eficacia en el tratamiento y cierre de anomalías identificadas en el marco de la seguridad y privacidad de la información, garantizando la mitigación de riesgos y la mejora continua del SGSI. Nota: Los incidentes serán identificados a través de reportes realizados por los usuarios o de resultados de las auditorías programadas para el sistema.

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

11. ANEXOS

Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

[Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas. Ministerio de tecnologías de la información y las comunicaciones. MSPPI. Versión 5. 21/04/2025.](#)

[Portal Gobierno Digital – TIC. Estrategias / MSPI / Documentación relacionada](#)

12. DOCUMENTOS RELACIONADOS

Interno / Externo	Nombre	Código / Ubicación
Interno	Manual de políticas y estándares de seguridad informática	GTI-M-002
Interno	Política de tratamiento de riesgos de seguridad y privacidad de la información	GTI-PO-006

13. BIBLIOGRAFIA

- [Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones. Febrero 2021.](#)

	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GTI-PO-005	
		Fecha de entrada en vigencia: 19/01/2026	
		Versión 04	

- [Plan de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones. Versión 10. 2025](#)
- **Banco Popular** (2024). Pautas de Seguridad
- **Banco BBVA** (2024). Seguridad para clientes

CONTROL DE CAMBIOS Y REVISIONES				
Revisión	Fecha	Versión Anterior	Versión Actual	Cambio Realizado
	11/01/2024		01	Se realiza el plan de seguridad de la información para el 2024 al 2027
01	21/10/2024	01	02	Se adicionan las buenas prácticas de seguridad para la parte bancaria
02	31/12/2024	02	03	Cambio en el cronograma de implementación del ciclo PHVA
03	19/01/2026	03	04	- Se actualiza la normatividad asociada - Se actualizan las definiciones - Se definen expresamente roles y responsabilidades - Se actualiza el punto 6 de talento humano requerido con la especificidad del perfil - Se actualiza el punto 7 de Materiales, insumos y equipos requeridos - Se actualiza el Plan de trabajo para la implementación del modelo del sistema de gestión de seguridad de la información en el marco del ciclo PHVA. - Se incluye herramienta de autodiagnóstico realizado - Se ajusta la ficha del indicador

Elaboró:	Revisó:	Aprobó:
Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información	Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información Carmen Rocío Camargo Acosta Contratista profesional apoyo Gestión de Calidad y Planeación	Natali Mosquera Narváez Gerente General