


**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

 E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRÁ	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**EMPRESA SOCIAL DEL ESTADO  
HOSPITAL REGIONAL DE CHIQUINQUIRÁ  
DEPARTAMENTO DE BOYACÁ**

**PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**CHIQUINQUIRÁ, ENERO 2026**



**E.S.E. HOSPITAL REGIONAL DE  
CHIQUINQUIRÁ**

CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN**

**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

**Contenido**

1.	Introducción.....	4
2.	Justificación.....	5
3.	Identificación.....	6
4.	Marco legal.....	7
5.	Definiciones y Conceptos.....	8
6.	Generalidades.....	13
7.	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ....	15
7.1.	Estado Actual de la Entidad Respecto al Sistema de Gestión de Seguridad de la Información .....	15
7.2.	Política de Seguridad de la Información.....	16
7.3.	Organización de la seguridad de la información.....	16
7.4.	Control de acceso.....	16
7.5.	Seguridad de las operaciones.....	17
7.6.	Gestión de incidentes de seguridad de la información.....	17
7.7.	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.....	17
7.8.	Relaciones con los proveedores.....	18
7.9.	Roles y responsabilidades.....	19
7.10.	Estrategias de seguridad digital.....	21
7.11.	Descripciones de las estrategias específicas.....	22
7.12.	Portafolio de proyectos.....	23
8.	Análisis Integral DOFA.....	26
9.	Recursos Necesarios y Presupuesto Estimado.....	27
10.	Recomendaciones.....	27
11.	Documentos Relacionados del Sistema Integrado de Gestión.....	28
12.	Indicadores de Éxito.....	29
13.	Actividades y Cronograma.....	30

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**

CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**


14.	Seguimiento y Evaluación.....	31
15.	Bibliografía.....	32
13.	Revisión y aprobación.....	32
14.	Control de Cambios al Documento.....	33

**Tabla de contenido de Tablas**

Tabla 1 Roles y Responsabilidades.....	19
Tabla 2 Estrategias específicas.....	22
Tabla 3 Portafolio de proyectos.....	24
Tabla 4 cronograma de proyectos.....	30

**Tabla de contenido de ilustraciones**

Ilustración 1 Instrumento autodiagnóstico de seguridad y privacidad de la información.....	15
Ilustración 2 Estrategias MINTIC.....	22

 E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRÁ	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

## 1. Introducción

La E.S.E. Hospital Regional de Chiquinquirá ratifica su compromiso con la protección de la información como un activo estratégico fundamental para el logro de sus objetivos misionales, estratégicos y operativos. En este marco, impulsa acciones transversales orientadas a prevenir el acceso no autorizado, el uso indebido, la divulgación, la interrupción o la destrucción de la información, garantizando la seguridad y privacidad de los datos generados en el desarrollo de su operación, en estricto cumplimiento de la normativa vigente y de las mejores prácticas internacionales.

El Plan de Seguridad y Privacidad de la Información tiene como propósito principal garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en la entidad, asegurando la protección de los datos personales y organizacionales a través del uso responsable y seguro de las Tecnologías de la Información y las Comunicaciones (TIC).

Este documento se constituye como una herramienta orientadora para la gestión de los procesos estratégicos, misionales, de apoyo y de evaluación, al establecer lineamientos claros para la adopción e implementación de controles de seguridad, promoviendo una cultura organizacional basada en la responsabilidad, la transparencia y el compromiso de todos los actores institucionales.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**CÓDIGO **3.3.2.D02**VERSIÓN **07**

FECHA Enero 30 de 2026

TIPO PLAN


PROCESO **GESTION DE RECURSOS LOGISTICOS****PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

## 2. Justificación

La Elaboración del Plan de Seguridad y Privacidad de la Información para la vigencia 2026 obedece a la necesidad de fortalecer la gestión de los activos de información de la E.S.E. Hospital Regional de Chiquinquirá, en un contexto de creciente dependencia de las Tecnologías de la Información, aumento de los riesgos digitales y mayores exigencias normativas en materia de protección de datos, transparencia y seguridad de la información.


La información constituye un activo estratégico para la continuidad de los procesos asistenciales, administrativos y financieros de la entidad; por tanto, su pérdida, alteración, uso indebido o indisponibilidad puede generar impactos operativos, legales y reputacionales significativos. En este sentido, el Plan se concibe como un instrumento de planeación y control que permite identificar, evaluar y tratar de manera sistemática los riesgos de seguridad de la información.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**3. Identificación**

<b>PROCESO</b>	<b>GESTIÓN DE RECURSOS LOGÍSTICOS</b>
<b>SUBPROCESO</b>	Tecnologías de la Información y las comunicaciones
<b>OBJETIVO GENERAL</b>	Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la ESE Hospital Regional de Chiquinquirá hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento.
<b>OBJETIVOS ESPECÍFICOS</b>	<ul style="list-style-type: none"> <li>➤ Definir y establecer la estrategia de seguridad digital de la entidad.</li> <li>➤ Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.</li> <li>➤ Priorizar los proyectos a implementar para la correcta implementación del SGSI.</li> <li>➤ Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.</li> </ul>
<b>ALCANCE</b>	El Plan de Seguridad y Privacidad de la Información aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la E.S.E. Hospital Regional de Chiquinquirá, así como a todos los funcionarios, contratistas, proveedores y terceros que, en el ejercicio de sus funciones, accedan, administren, procesen, almacenen, transmitan o custodien activos de información de la entidad, independientemente del medio o soporte utilizado (físico, digital o electrónico).
<b>RESPONSABLES</b>	Líder de tecnologías, Coordinador de Planeación, Gestión documental, Subgerencia Administrativa, Control Interno.

	CÓDIGO	3.3.2.D02	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	07	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

#### 4. Marco legal

**Ley 1712 de 2014**, Art 4. 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.

**Norma Técnica ISO/IEC 27000**. 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.


**Ley 1581 de 2012, Art 3**. Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

**Ley 1581 de 2012, Art 3**. Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

**Decreto 1377 de 2013**, 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 1499 de 2017** Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.

**Modelo de Seguridad y Privacidad de la Información**, Versión 3.0.2, 2016.  
MinTIC.

	CÓDIGO	3.3.2.D02	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	07	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

## 5. Definiciones y Conceptos

**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).

**Activos de información:** Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos. 1 en cuanto a 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).

**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).


**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)

**Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para 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)

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**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).

**Ciberespacio:** 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 interacción entre usuarios. (Resolución CRC 2258 de 2009).

**Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal 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.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	3.3.2.D02	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	07	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**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).

**Disponibilidad:** Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.

**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)


**Evento de seguridad de la información:** Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.

**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).

**Guía:** Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

**Incidente de seguridad de la información:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	3.3.2.D02	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	07	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

**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)

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

**Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

**MSPI:** Modelo de Seguridad y Privacidad de la Información

**Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.


**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 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).

**Parte interesada:** (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**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.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	3.3.2.D02	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	07	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

Propietario/responsable de activo de información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

**Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

**Procedimiento:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

**Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

**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).

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

**Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

**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).

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**6. Generalidades**

El Plan de Seguridad y Privacidad de la Información se desarrolla como un instrumento institucional de planeación, gestión y control, orientado a establecer las directrices generales para la protección de los activos de información de la E.S.E. Hospital Regional de Chiquinquirá. Su aplicación se fundamenta en el cumplimiento de la normatividad vigente, las políticas internas y las buenas prácticas en seguridad de la información.

Las generalidades del Plan consideran los siguientes lineamientos:

**Enfoque basado en riesgos**

La seguridad de la información se gestiona bajo un enfoque preventivo, mediante la identificación, análisis, valoración y tratamiento de los riesgos asociados a los activos de información, priorizando aquellos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

**Articulación con el Sistema Integrado de Gestión y el MIPG**

El Plan se integra al Sistema Integrado de Gestión de la entidad y al Modelo Integrado de Planeación y Gestión (MIPG), asegurando coherencia con los procesos, el control interno, la gestión documental y la mejora continua.

**Alineación normativa y técnica**

Las disposiciones del Plan se encuentran alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, la norma ISO/IEC 27001 y la normativa aplicable en materia de protección de datos personales, transparencia y acceso a la información pública.

**Definición de roles y responsabilidades**

Se establecen responsabilidades claras para la alta dirección, líderes de proceso, áreas de apoyo, funcionarios y contratistas, con el fin de garantizar la adecuada implementación, operación y seguimiento de los controles de seguridad de la información.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**CÓDIGO **3.3.2.D02**VERSIÓN **07**

FECHA Enero 30 de 2026

TIPO PLAN

PROCESO **GESTION DE RECURSOS LOGISTICOS****PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ****Aplicación de controles administrativos y tecnológicos**

La protección de la información se soporta en la implementación de controles administrativos, técnicos y físicos, tales como políticas, procedimientos, gestión de accesos, copias de seguridad, seguridad perimetral y monitoreo de la infraestructura tecnológica.

**Gestión de incidentes y continuidad del negocio**

El Plan contempla lineamientos generales para la gestión de incidentes de seguridad de la información y la continuidad del negocio, orientados a minimizar el impacto de eventos adversos sobre la operación institucional.

**Sensibilización y cultura organizacional**

Se promueve la capacitación y sensibilización permanente del personal como elemento transversal para el fortalecimiento de la cultura de seguridad y privacidad de la información.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**



E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**

CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN**

**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

**7. PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN**

**7.1. Estado Actual de la Entidad Respecto al Sistema de Gestión de Seguridad de la  
Información**

La ESE Hospital Regional de Chiquinquirá ha avanzado en la implementación de controles dentro del Sistema de Gestión de Seguridad de la Información (SGSI), Actualmente se encuentra en una etapa de consolidación y mejora continua. El avance actual de la entidad refleja una etapa intermedia en la madurez del SGSI, caracterizada por el establecimiento de procesos básicos y el desarrollo de controles fundamentales. Sin embargo, es necesario implementar de manera progresiva los controles restantes, reforzar la documentación de los mismos y asegurar su alineación con las mejores prácticas internacionales y las normativas del Modelo de Seguridad y Privacidad de la Información (MSPI).

*Ilustración 1 Instrumento autodiagnóstico de seguridad y privacidad de la información*



Fuente: Instrumento de Evaluación MSPI

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**CÓDIGO **3.3.2.D02**VERSIÓN **07**

FECHA Enero 30 de 2026

TIPO PLAN

PROCESO **GESTION DE RECURSOS LOGISTICOS****PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ****7.2. Política de Seguridad de la Información**

La política de seguridad de la información ha sido documentada y adoptada por la alta dirección, pero su implementación efectiva a nivel operativo aún presenta áreas de oportunidad. Aunque la política está alineada con las normativas ISO 27001, se requiere un fortalecimiento en su divulgación y la realización de capacitaciones periódicas para todo el personal, con el fin de garantizar una comprensión plena y su aplicación efectiva.

Se proyecta la optimización de la política mediante la integración de procesos automáticos de monitoreo y revisión, buscando una mejora continua. Se desarrollarán mecanismos de retroalimentación para asegurar que los controles de seguridad sean constantemente actualizados y mejorados en función de las amenazas emergentes.

**7.3. Organización de la seguridad de la información**

Actualmente, la organización ha reconocido la necesidad de un enfoque estructurado para la gestión de la seguridad de la información. No obstante, los roles y responsabilidades en términos de seguridad aún requieren una mayor formalización y asignación. Existen algunos avances en la designación de los responsables de los controles, pero no todos los procesos están claramente definidos ni formalmente implementados.


Se proyecta implementar un modelo de gobernanza más robusto, con una asignación clara de responsabilidades y autoridad en materia de seguridad de la información, apoyado por una estructura organizacional sólida. Este proceso estará acompañado de un sistema de gestión que facilite la integración de controles y la rendición de cuentas.

**7.4. Control de acceso**

Ha sido implementado de manera básica en la entidad, pero aún persisten brechas en su formalización y en la capacitación continua del personal. Los controles de acceso se encuentran establecidos de manera parcial, y se necesita asegurar su aplicación en todos los puntos críticos de la infraestructura.

Se tiene como objetivo alcanzar un nivel de madurez más alto en los controles de acceso, adoptando tecnologías de autenticación multifactor y reforzando la gestión de

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

identidades. Se desarrollará un plan de implementación que garantice la alineación de estos controles con las políticas de seguridad establecidas, contribuyendo a la optimización del acceso seguro a los recursos y sistemas de la entidad.

### **7.5. Seguridad de las operaciones**

En términos de seguridad de las operaciones, la entidad ha realizado esfuerzos en establecer procedimientos básicos, aunque su aplicación no es completamente uniforme. La falta de procedimientos estandarizados en todas las áreas ha resultado en una implementación variable de las mejores prácticas en la protección de los sistemas y la información.

Se implementarán procedimientos estandarizados para la seguridad de las operaciones en todas las áreas, garantizando su cumplimiento y reforzando la protección de las infraestructuras críticas. A través de auditorías internas y herramientas de monitoreo, se garantizará que todos los procesos sean controlados y revisados constantemente.

### **7.6. Gestión de incidentes de seguridad de la información**

La gestión de incidentes de seguridad está en una fase inicial, con procedimientos básicos que no están completamente formalizados ni aplicados de manera consistente. Existen mecanismos reactivos en lugar de proactivos.

Se planea implementar un plan integral de gestión de incidentes que contemple la identificación, análisis, respuesta y cierre de incidentes de forma eficiente. El objetivo es establecer un sistema de gestión de incidentes más avanzado, apoyado por herramientas de monitoreo en tiempo real y la capacitación constante del personal.

### **7.7. Aspectos de seguridad de la información en la gestión de la continuidad del negocio**

La entidad ha comenzado a abordar los aspectos de seguridad de la información dentro del marco de la gestión de la continuidad del negocio, pero aún carece de una planificación integral y de un enfoque completo para los eventos disruptivos.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**CÓDIGO **3.3.2.D02**VERSIÓN **07**

FECHA Enero 30 de 2026

TIPO PLAN

PROCESO **GESTION DE RECURSOS LOGISTICOS****PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

En las siguientes vigencias, se implementará una estrategia de continuidad del negocio que incluirá planes de recuperación ante desastres, respaldados por pruebas periódicas y simulacros. Se integrarán los aspectos de seguridad de la información en todos los niveles del plan de continuidad para minimizar los riesgos y garantizar la resiliencia organizacional.


### **7.8. Relaciones con los proveedores**

En cuanto a la seguridad de la información se encuentra en una etapa inicial, sin procedimientos estandarizados ni acuerdos formalizados que definan los requisitos de seguridad con los proveedores.

Se establecerán contratos de servicios que incluyan cláusulas específicas sobre seguridad de la información y se formalizarán las relaciones con los proveedores. A través de auditorías de seguridad y revisiones periódicas, se garantizará que los proveedores cumplan con los estándares de seguridad establecidos por la entidad.

La entidad se encuentra en una fase intermedia de madurez en cuanto al Sistema de Gestión de Seguridad de la Información, con un enfoque en la documentación y la implementación de controles fundamentales. En las próximas vigencias, se prevé un esfuerzo continuo para fortalecer los controles existentes, optimizar las prácticas actuales y formalizar la documentación necesaria para cumplir con los estándares internacionales de seguridad de la información. Este proceso estará basado en la mejora continua y la capacitación del personal, con un enfoque estratégico hacia la implementación y optimización del SGSI, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC y las normativas ISO.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**7.9. Roles y responsabilidades**

La ESE Hospital Regional de Chiquinquirá define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad

*Tabla 1 Roles y Responsabilidades*

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
<b>Alta Dirección</b>	<ul style="list-style-type: none"> <li>*Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).</li> </ul>
<b>Comité de Gestión y Desempeño</b>	<ul style="list-style-type: none"> <li>*Aprobar y hacer seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI</li> <li>* Aprobar los recursos necesarios para la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información.</li> <li>* Conocer los resultados de los estudios, análisis y recomendaciones en materia de seguridad y privacidad de la información y generar las recomendaciones necesarias.</li> </ul>
<b>Tecnologías de la Información y las comunicaciones (TIC)</b>	<ul style="list-style-type: none"> <li>*Liderar las acciones necesarias para establecer, implementar, mantener y mejorar la Seguridad de la Información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información MSPI, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.</li> <li>*Conformar y liderar el equipo de respuesta a emergencias informáticas y centros de operaciones de seguridad con el fin de apoyar la gestión de incidentes de seguridad informática que se llegasen a presentar en la ESE Hospital Regional de Chiquinquirá.</li> <li>* Implementar y gestionar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.</li> <li>* Establecer, verificar, monitorear y validar los procedimientos de continuidad y de contingencia para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.</li> <li>*Establecer, documentar y dar mantenimiento a los procedimientos de seguridad de la información que apliquen</li> </ul>

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**




CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

	<p>para la plataforma de tecnologías de información administrada por esta unidad.</p> <p>*Analizar, definir, documentar y gestionar el plan de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobadas por la ESE Hospital Regional de Chiquinquirá.</p> <p>*Elaborar los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información en la ESE Hospital Regional de Chiquinquirá y presentarlos para aprobación</p> <p>*Elaborar y/o Actualizar el Plan de Sensibilización y Comunicación en Seguridad de la Información.</p> <p>* Verificar las actividades de monitoreo del uso de los activos de información para prevenir el impacto de los riesgos derivados de pérdida de integridad, disponibilidad y confidencialidad de la información.</p> <p>*Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la ESE Hospital Regional de Chiquinquirá.</p>
<b>Talento Humano</b>	<p>*Asegurar que los empleados, Terceros, contratistas reciban la ruta de capacitación sobre sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.</p> <p>* Gestionar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente.</p>
<b>Control Interno</b>	<p>*Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.</p> <p>*Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.</p>
<b>Comunicación Interna y externa</b>	<p>*Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.</p>
	<p>*Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad.</p>

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

<b>Gestión Jurídica y contractual</b>	<p>*Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.</p> <p>*Brindar asesoría a los procesos de la ESE en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.</p> <p>*Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.</p> <p>*Asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.</p>
<b>Líderes de Proceso</b>	<p>*Implementar y dar cumplimiento de las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).</p>
<b>Todos los funcionarios y contratistas</b>	<p>* Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos</p> <p>*Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.</p> <p>*Reportar de manera inmediata y a través de los canales establecidos la sospecha u ocurrencia de eventos considerados incidentes de seguridad de la información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad de la Información.</p>

**7.10. Estrategias de seguridad digital**

La estrategia de seguridad digital de la ESE Hospital Regional de Chiquinquirá se fundamenta en la planificación estratégica de la seguridad, integrando la gestión de riesgos en los procesos organizacionales y priorizando la protección de los activos de información críticos. Para ello, se implementa un Sistema de Gestión de Seguridad de la Información (SGSI) alineado al ciclo PHVA de la ISO 27001, asegurando controles efectivos y cumplimiento normativo.

Se promueve la interoperabilidad y la privacidad por diseño en todas las plataformas y sistemas, garantizando la protección de los datos sensibles de las víctimas

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**



E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**

CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

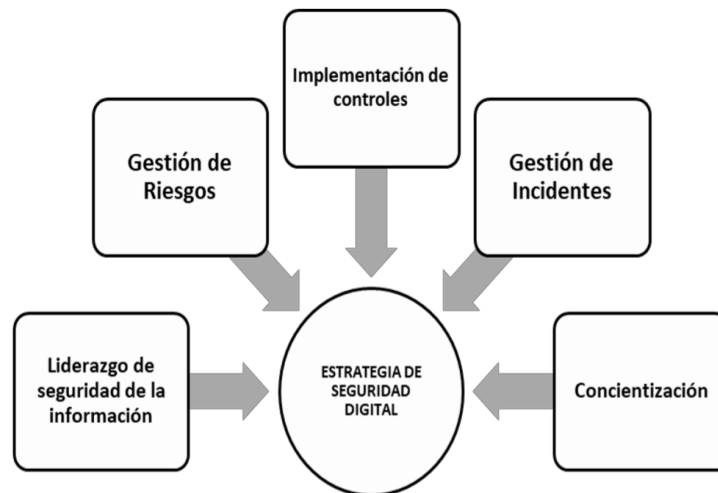
**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

bajo el Modelo de Seguridad y Privacidad de la Información (MSPI). Además, se establecen procedimientos sólidos para la gestión de incidentes de seguridad y la continuidad del negocio, asegurando la operación ininterrumpida mediante planes de recuperación alineados a estándares internacionales.

La estrategia incluye la capacitación continua del personal para fomentar una cultura organizacional que priorice la seguridad de la información.

*Ilustración 2 Estrategias MINTIC*



Fuente: MINTIC

**7.11. Descripciones de las estrategias específicas**

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

*Tabla 2 Estrategias específicas*

<b>ESTRATEGIA / EJE</b>	<b>DESCRIPCIÓN/OBJETIVO</b>
<b>Liderazgo de seguridad de la información</b>	Asegurar que se establezca el Modelo de

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**



E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**

CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN**


**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

	Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
<b>Gestión de riesgos</b>	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
<b>Concientización</b>	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
<b>Implementación de controles</b>	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
<b>Gestión de incidentes</b>	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Fuente: Propia

**7.12. Portafolio de proyectos**

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

Para cada estrategia específica, la ESE define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

*Tabla 3 Portafolio de proyectos*

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
<b>Liderazgo de seguridad de la información</b>	*Actualizar e implementar una política de seguridad.	*Política de Seguridad Formalizada e Implementada.
	*Definición de Roles y Responsabilidades de Seguridad de la Información.	*Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados.
	*Adopción de políticas para la virtualización y gestión de sistemas críticos.	*Políticas para la operación de sistemas virtualizados.
<b>Gestión de riesgos</b>	*Identificar, valorar y clasificar los riesgos asociados a los activos de información.	*Matriz de riesgos de seguridad digital.
	* Definir planes de tratamiento de riesgos de seguridad.	*Plan de tratamiento de riesgos.
	*Contratación del servicio de Ethical Hacking y Pentesting.	*Reporte de vulnerabilidades identificadas. *Implementación de recomendaciones para mitigación.
<b>Concientización</b>	* Plan de Comunicación y sensibilización de Seguridad de la Información.	*Módulos de capacitación pregrabados en Classroom. *Registro de asistencia.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**



E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**

CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>


**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN**

**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

	*Contratación de servicio de seguridad perimetral (Firewall).	*Firewall con licencias activas implementado.  *Infraestructura protegida con conexión segura entre sedes.
	*Adquisición de licencias de antivirus para equipos y servidores.	*Antivirus actualizado en todos los equipos.
	*Proyecto de Adecuación del Datacenter.	*Adecuación de área de trabajo (Iluminación, Puerta hermética, Sensores de Temperatura Humedad, Sensor Biométrico de apertura y botón de pánico, cámara registro de acceso).
<b>Gestión de incidentes</b>	Actualizar e implementar Procedimiento de gestión de incidentes de seguridad	Procedimiento de gestión de incidentes de seguridad formalizado.

Fuente: Propia

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**8. Análisis Integral DOFA**

FORTALEZAS (ANÁLISIS INTERNO)		DEBILIDADES (ANÁLISIS INTERNO)	
1	Existencia de un Plan de Seguridad y Privacidad de la Información formalmente definido y actualizado para la vigencia 2026.	1	Nivel de madurez intermedio del Sistema de Gestión de Seguridad de la Información, con controles aún en proceso de consolidación
2	Compromiso de la alta dirección y articulación del plan con el Sistema Integrado de Gestión y el MIPG.	2	Brechas en la apropiación y aplicación operativa de las políticas de seguridad de la información por parte del personal
3	Identificación de roles y responsabilidades institucionales en materia de seguridad de la información	3	Limitaciones en recursos tecnológicos y financieros para la implementación inmediata de todos los controles definidos
4	Alineación del SGSI con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001	4	Gestión de incidentes de seguridad con un enfoque mayormente reactivo y en proceso de formalización
5	Disponibilidad de procedimientos, políticas y controles documentados asociados a la gestión de tecnologías de la información	5	Necesidad de fortalecer la estandarización y documentación de controles en todos los procesos institucionales.
OPORTUNIDADES (ANÁLISIS EXTERNO)		AMENAZAS (ANÁLISIS EXTERNO)	
1	Lineamientos y acompañamiento técnico del Ministerio TIC a través del MSPI y la Política de Gobierno Digital	1	Incremento de ciberamenazas y ataques informáticos dirigidos a entidades del sector salud.
2	Disponibilidad de buenas prácticas y estándares internacionales en seguridad de la información aplicables al sector salud.	2	Riesgos asociados al tratamiento de datos personales sensibles y a posibles sanciones por incumplimiento normativo
3	Avances tecnológicos que facilitan la implementación de controles de seguridad, monitoreo y respaldo de la información	3	Dependencia creciente de plataformas tecnológicas para la prestación de los servicios de salud
4	Fortalecimiento de la cultura de seguridad digital a nivel nacional en el sector público	4	Fallas de servicios tecnológicos o de terceros que pueden afectar la disponibilidad de la información

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**



CÓDIGO	<b>3.3.2.D02</b>
VERSIÓN	<b>07</b>
FECHA	Enero 30 de 2026
TIPO	PLAN
PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

<b>5</b>	Posibilidad de articulación con planes institucionales como el PETI y el Plan de Continuidad del Negocio	<b>5</b>	Cambios constantes en el marco normativo y en los requisitos de los entes de control
----------	--	----------	--

**9. Recursos Necesarios y Presupuesto Estimado**


RECURSO	ACTIVIDAD	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Equipos y Software	EQUIPOS DE CÓMPUTO SCANNER Y VIDEO BEAM RENOVACIÓN		\$	\$ 180.000.000
Equipos y Software	LICENCIAS UTM SEGURIDAD PERIMETRAL ANUAL		\$	\$ 100.000.000
Equipos y Software	SERVICIO DE ETHICAL HACKING		\$	\$25.000.000
Equipos y Software	COPIAS DE SEGURIDAD		\$	\$28.800.000
Equipos y Software	LICENCIAS ANTIVIRUS		\$	\$ 95.000.000
<b>TOTAL:</b>				\$ 428.800.000

**10. Recomendaciones**

Durante el desarrollo y ejecución del Plan de Seguridad y Privacidad de la Información, se recomienda tener en cuenta los siguientes puntos de control:

- ✓ Garantizar el compromiso permanente de la alta dirección y la asignación de los recursos necesarios para la implementación de las acciones definidas.
- ✓ Actualizar periódicamente la identificación y valoración de los riesgos de seguridad de la información, conforme a cambios tecnológicos y normativos.
- ✓ Asegurar la divulgación, comprensión y cumplimiento de las políticas y procedimientos de seguridad de la información por parte de funcionarios y contratistas.
- ✓ Aplicar de manera formal el procedimiento de gestión de incidentes de seguridad de la información y documentar los eventos ocurridos.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

- ✓ Verificar el cumplimiento de los requisitos de seguridad de la información en la gestión con proveedores y terceros.
- ✓ Realizar seguimiento y evaluación continua al cumplimiento del Plan.

### 11. Documentos Relacionados del Sistema Integrado de Gestión

- 3.3.2. D01 PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION.
- 3.3.2. P01 F01 MANTENIMIENTO PREVENTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA.
- 3.3.2. P01 F02 MANTENIMIENTO PREVENTIVO DE IMPRESORAS Y SCANNER
- 3.3.2. P02 F01 MANTENIMIENTO CORRECTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA
- 3.3.2. P07 F01 RECEPCIÓN DE SERVICIO DE SISTEMAS
- 3.3.2.P19 F01 REGISTRO DE VARIACIONES EN LOS SISTEMAS DE INFORMACION
- 3.3.2.D03 PLAN DE DATOS ABIERTOS
- 3.3.2.R01 ADMINISTRACION Y CONTROL DE LICENCIAS
- 3.3.2.P03 COPIA DE SEGURIDAD DEL SISTEMA DGH
- 3.3.2.P04 COPIA DE SEGURIDAD DEL SISTEMA SAIH3.3.2.P05 INSTALACION DE LOS MODULOS DEL SISTEMA SAIH
- 3.3.2.P06 CREACION DE REPORTES DEL SISTEMA DGH
- 3.3.2.P07 INSTALACION Y CREACION DE USUARIOS DE DGH
- 3.3.2.P08 RECUPERACIÓN DE DATOS DEL SISTEMA DGH
- 3.3.2.P09 BAJA DE SOFTWARE
- 3.3.2.P10 ENTREGA O CAMBIO DE EQUIPOS TECNOLOGICOS
- 3.3.2.P11 DILIGENCIAMIENTO DE LA HOJA DE VIDA DE LOS EQUIPOS TECNOLOGICOS
- 3.3.2.P12 ADMINISTRACIÓN DEL ANTIVIRUS
- 3.3.2.P13 CONTROL EN LA RED LAN E INTERNET POR UTM

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**E.S.E. HOSPITAL REGIONAL DE  
**CHIQUINQUIRÁ**CÓDIGO **3.3.2.D02**VERSIÓN **07**

FECHA Enero 30 de 2026

TIPO PLAN


PROCESO **GESTION DE RECURSOS LOGISTICOS****PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**

- 3.3.2.P14 MANTENIMIENTO PREVENTIVO AL SISTEMA DGH
- 3.3.2.P15 REGISTRO DE USUARIOS Y ASIGNACIÓN DE PERMISOS EN EL SISTEMA  
DGH
- 3.3.2.P16 MANTENIMIENTO CORRECTIVO AL SISTEMA SAIH
- 3.3.2.P17 REGISTRO DE USUARIOS Y PERMISOS EN EL SISTEMA SAIH
- 3.3.2.P18 REGISTRO DE USUARIOS Y PERMISOS EN EL SISTEMA SGE
- 3.3.2.P19 ANALISIS Y DETECCION DE VARIACIONES EN LOS SISTEMAS DE  
INFORMACION
- 3.3.2. T02 CARACTERIZACIÓN SUBPROCESO TECNOLOGÍAS DE INFORMACIÓN  
Y LAS COMUNICACIONES Subproceso Tecnologías de Información y las Comunicaciones

**12. Indicadores de Éxito**

<b>RESULTADO/PRODUCTO ESPERADO</b>	<b>INDICADOR</b>
Nº de actividades realizadas y aprobadas por la alta dirección.	Cumplimiento (%)=(Numero total de actividades programadas/Numero de actividades completadas)×100

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**

	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			


### 13. Actividades y Cronograma

Desde el área de tecnologías de la Información se presenta el cronograma de proyectos y operaciones establecidos en el marco del plan estratégico de seguridad de la Información – PESI, Alineado con el Plan Estratégico de Tecnologías de la Información.

*Tabla 4 cronograma de proyectos*

Nº	ASPECTOS/ CRITERIOS	ACTIVIDAD	META	SOPORTE	RESPONSABLE	FECHA PROGRAMADA
1	Plan PESI	Definición de Roles y Responsabilidades de Seguridad de la Información.	100%	Informe de resultados	Líder Tecnologías de la Información	28 / 06 / 2026
3	Plan PESI	Contratación de servicio de seguridad perimetral (Firewall).	100%	Informe de resultados	Líder Tecnologías de la Información	28 / 03 / 2026
4	Plan PESI	Adquisición de licencias de antivirus para equipos y servidores.	100%	Informe de resultados	Líder Tecnologías de la Información	28 / 03 / 2026
5	Plan PESI	Plan de Comunicación y sensibilización de Seguridad de la Información.	100%	Informe de resultados	Líder Tecnologías de la Información	28 / 06 / 2025
7	Plan PESI	Simulacros de pruebas de continuidad del negocio.	100%	Informe de resultados	Líder Tecnologías de la Información	30 / 06 / 2025
8	Plan PESI	Actualizar e implementar la política de seguridad	100%	Informe de resultados	Líder Tecnologías de la Información	29 / 09 / 2026
9	Plan PESI	Proyecto de	90%	Informe de resultados	Líder	29 / 09 / 2026

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**


	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

		Adecuación del Datacenter			Tecnologías de la Información	
<b>10</b>	Plan PESI	Contratación del servicio de Ethical Hacking y Pentesting.	70% de los usuarios	Informe de resultados	Líder Tecnologías de la Información	29 / 09/ 2026
<b>11</b>	Plan PESI	Identificar, valorar y clasificar los riesgos asociados a los activos de información	50%	Informe de resultados	Líder Tecnologías de la Información	29 / 09/ 2026
<b>12</b>	Plan PESI	Actualizar e implementar Procedimiento de gestión de incidentes de seguridad	100%	Informe de resultados	Líder Tecnologías de la Información	29 / 09/ 2026
<b>13</b>	Plan PESI	Adopción de políticas para la virtualización y gestión de sistemas críticos.	50 %	Informe de resultados	Líder Tecnologías de la Información	29 / 12 / 2026
<b>14</b>	Plan PESI	Definir planes de tratamiento de riesgos de seguridad	100%	Informe de resultados	Líder Tecnologías de la Información	29 12 /2026

**14. Seguimiento y Evaluación**

El presente plan se sustentará en el **Comité de Gestión y Desempeño** de forma anual por parte del responsable de la proyección del documento, mediante indicadores, con la presentación de los casos de éxito producto de las actividades.

**SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS**


	CÓDIGO	<b>3.3.2.D02</b>	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>
	VERSIÓN	<b>07</b>	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	<b>GESTION DE RECURSOS LOGISTICOS</b>	
<b>USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ</b>			

**15. Bibliografía**

No.	DOCUMENTO
1	Modelo de Seguridad y Privacidad de la Información (MSPI) (S/f-c). Gov.co. Recuperado el 29 de enero de 2025, de <a href="https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf">https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf</a>
2	Política de Gobierno Digital. (s/f). Gov.co. Recuperado el 29 de enero de 2025, de <a href="https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/">https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/</a>
3	Guía MINTIC PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (S/f-d). Gov.co. Recuperado el 29 de enero de 2025, de <a href="https://mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_2024_20240125.pdf">https://mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_2024_20240125.pdf</a>

**13. Revisión y aprobación**

ÍTEM	ELABORÓ	COORDINADOR	REVISÓ	APROBÓ
<b>Firma</b>				
<b>Nombre</b>	Karem Dayanna López	Jonathan García	Luber Ney Murcia	Juliana del Pilar Cortázar Murillo
<b>Cargo</b>	Profesional Administrativo de Tecnologías de la información	Líder Tecnologías de la Información	Coordinador de Planeación Estratégica	Gerente
<b>Fecha</b>	Ene. 30 de 2026	Ene. 30 de 2026	Ene. 30 de 2026	Ene. 30 de 2026

SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS			
	CÓDIGO	3.3.2.D02	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	07	
	FECHA	Enero 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

#### 14. Control de Cambios al Documento

Fecha del Cambio	Versión Actual	Justificación del Cambio	Indique el ítem del Documento Donde se Requiere el Cambio	Versión Nueva	Nombre y Cargo de Quien Elaboro el Cambio	Nombre y Cargo de Quien Aprobó el Cambio
Ene. 28 de 2022	3	Actualización anual	En todo el documento teniendo en cuenta las nuevas metas del área.	4	Rosbelth Gaona Líder Tecnologías de la Información	Liseth Cañon Subgerente Administrativa y Financiera
Ene. 28 de 2023	4	Actualización anual	En todo el documento teniendo en cuenta las nuevas metas del área.	5	Jonathan García Líder Tecnologías de la Información	Mauricio Zambrano Subgerente Administrativa y Financiera
Ene. 28 de 2024	5	Actualización anual	En todo el documento teniendo en cuenta las nuevas metas del área.	6	Jonathan García Líder Tecnologías de la Información	Mauricio Zambrano Subgerente Administrativa y Financiera
Ene. 28 de 2025	6	Actualización anual	En todo el documento teniendo en cuenta las nuevas metas del área.		Jonathan García Líder Tecnologías de la Información	Juliana del Pilar Cortázar Murillo Gerente