

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



CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

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

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

CHIQUINQUIRÁ ENERO 2026


	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

Tabla de Contenido

1.	Introducción.....	4
2.	Justificación.....	5
3.	Identificación	6
4.	Marco legal.....	7
5.	Definiciones y Conceptos	8
7.	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	10
7.1.	Contexto para la Gestión del Riesgo de Seguridad y Privacidad de la Información.	10
7.2.	Criterios de Evaluación del Riesgo:	10
7.3.	Criterios de Impacto.....	11
7.4.	Criterios de Aceptación del Riesgo.....	11
7.5.	Identificación de Activos de la Información.....	12
7.6.	Riesgos de Tecnologías de la Información y Comunicaciones	15
7.6.1.	Análisis de Riesgos.....	15
7.7.	Controles.....	17
7.7.1.	Determinación de Controles.....	17
8.	Análisis Integral DOFA	21
9.	Recursos Necesarios y Presupuesto Estimado.....	22
10.	Recomendaciones.....	22
11.	Documentos Relacionados del Sistema Integrado de Gestión.....	23
12.	Indicadores de Éxito	25
13.	Actividades y Cronograma	25
14.	Seguimiento y Evaluación.....	26
15.	Bibliografía	26
16.	Revisión y aprobación	26



E.S.E. HOSPITAL REGIONAL DE
CHIQUINQUIRÁ

CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

17. Control de Cambios al Documento27

Tabla de Ilustraciones

Ilustración 1 3.3.3. P04 F03 INVENTARIOS DE ACTIVOS DE LA INFORMACIÓN. 12

Ilustración 2 Criterios de clasificación..... 13

Ilustración 3 Niveles de clasificación. 13


Ilustración 4 Proceso para la administración del riesgo en seguridad de la información. 14

Ilustración 5 Tipología de Activos. (MINTIC) 15

Ilustración 6 Matriz de riesgos TIC. 16

Ilustración 7 Matriz de calor inherente 16

Ilustración 8 Mapa de Calor Residual..... 17

 E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRÁ	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			


1. Introducción

La información constituye uno de los activos estratégicos más relevantes para las organizaciones en la actualidad, especialmente para las entidades del sector salud, dado que la afectación de los principios de confidencialidad, integridad y disponibilidad puede generar impactos significativos de carácter operativo, asistencial, legal, financiero y reputacional. En este sentido, la E.S.E. Hospital Regional de Chiquinquirá reconoce la información como un activo fundamental para el cumplimiento de sus objetivos misionales, asistenciales, administrativos y de control, así como para la adecuada prestación de los servicios de salud.

En el marco de la transformación digital del Estado, la interoperabilidad de los sistemas de información en salud y el fortalecimiento de la seguridad digital, se hace necesaria la actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, incorporando un enfoque preventivo y proactivo, alineado con el Plan Estratégico de Tecnologías de la Información (PETI), la Política de Seguridad de la Información (PSI), el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información del Estado Colombiano.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece los lineamientos, controles, responsables y acciones orientadas a identificar, analizar, evaluar y tratar los riesgos asociados a la seguridad y privacidad de la información, conforme a la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP). De esta manera, se busca garantizar que la información institucional se mantenga confidencial, íntegra y disponible a lo largo de todo su ciclo de vida, desde su captura y almacenamiento hasta su uso, conservación y disposición final, asegurando la continuidad de los servicios y el cumplimiento de la normatividad vigente.

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

 E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRÁ	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

2. Justificación

La elaboración y actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se fundamenta en la necesidad de fortalecer la protección de uno de los activos más importantes de la E.S.E. Hospital Regional de Chiquinquirá: la información institucional, asistencial y administrativa. En el contexto del sector salud, la materialización de riesgos asociados a la pérdida, alteración o divulgación no autorizada de la información puede generar impactos significativos en la continuidad de la atención, el cumplimiento normativo, la sostenibilidad financiera y la reputación institucional.

El crecimiento en el uso de tecnologías de la información, la interoperabilidad de los sistemas de salud, la transformación digital del Estado y el aumento de amenazas cibernéticas hacen indispensable adoptar un enfoque sistemático, preventivo y proactivo para la gestión de los riesgos de seguridad y privacidad de la información. Este plan permite identificar, analizar, evaluar y tratar dichos riesgos de manera estructurada, estableciendo controles técnicos, administrativos y operativos proporcionales al nivel de exposición de los activos de información.

Asimismo, el Plan de Tratamiento de Riesgos constituye un instrumento clave para dar cumplimiento a la normatividad vigente, a los lineamientos del Modelo de Seguridad y Privacidad de la Información del Estado Colombiano, al Modelo Integrado de Planeación y Gestión (MIPG) y a la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública, fortaleciendo el Sistema de Control Interno y la gestión institucional basada en riesgos.

En este sentido, la implementación de los controles definidos contribuye a garantizar los principios de confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida, a proteger el recurso público, a asegurar la continuidad de los servicios de salud y a promover una cultura organizacional orientada a la seguridad de la información y la responsabilidad en su manejo por parte de todos los servidores y colaboradores de la entidad.

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



E.S.E. HOSPITAL REGIONAL DE
CHIQUINQUIRÁ


CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

3. Identificación

PROCESO	GESTIÓN DE RECURSOS LOGÍSTICOS
SUBPROCESO	Tecnologías de la Información y las comunicaciones
OBJETIVO GENERAL	Definir controles por medio de actividades y herramientas que permitan una adecuada gestión de los riesgos de seguridad y privacidad de la información <ul style="list-style-type: none"> ➤ Consolidar una administración de riesgos acorde con las necesidades de la institución. ➤ Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad. ➤ Sensibilizar al personal sobre de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
OBJETIVOS ESPECÍFICOS	
ALCANCE	<p>El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a los activos de información identificados, clasificados y valorados por la E.S.E. Hospital Regional de Chiquinquirá, asociados a los procesos misionales, estratégicos, de apoyo y de evaluación, que sean soportados por las Tecnologías de la Información y las Comunicaciones.</p> <p>El alcance del plan comprende la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, así como la definición e implementación de controles técnicos, administrativos y operativos, orientados a proteger la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida.</p> <p>La aplicación de los controles definidos será de obligatorio cumplimiento para los servidores públicos, contratistas y terceros que, en razón de sus funciones, administren, usen o tengan acceso a los activos de información institucionales.</p>
RESPONSABLES	Líder de tecnologías, Coordinador de Planeación, Gestión documental, Subgerencia Administrativa, Control Interno.

	CÓDIGO	3.3.2.D04	<p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

4. Marco legal

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.


Norma NTC / ISO 27001:2013: Tecnología de la Información. Técnicas de seguridad de la información y Código de Práctica para controles de seguridad de la información Página 7 de 18

Norma NTC/ISO 27002:2013: Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información

Norma NTC / ISO 31000:2009: Gestión de Riesgo, Principios y Directrices

Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

Modelo de Gestión de Riesgos de Seguridad Digital (**MGRSD**).

	CÓDIGO	3.3.2.D04	<p>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

5. Definiciones y Conceptos

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar su importancia.

Factor de riesgo: Agente ya sea humano o tecnológico que genera el riesgo.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud. Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Da el resultado en donde se ubica el riesgo por cada activo de información.



CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.


6. Generalidades

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. Hospital Regional de Chiquinquirá se desarrolla bajo un enfoque de gestión integral del riesgo, orientado a la protección de los activos de información institucionales y al aseguramiento de los principios de confidencialidad, integridad y disponibilidad a lo largo de todo su ciclo de vida.

Desde el punto de vista técnico y operativo, el plan contempla, entre otros, los siguientes aspectos generales:

- La adopción de una metodología estandarizada para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información.
- La definición e implementación de controles preventivos y correctivos, de naturaleza técnica, administrativa y organizacional, orientados a reducir la probabilidad de ocurrencia y el impacto de los riesgos identificados.
- El fortalecimiento de la seguridad de la infraestructura tecnológica, mediante la gestión de la obsolescencia, la aplicación de actualizaciones, parches de seguridad, mantenimiento preventivo y correctivo, y la adopción de mecanismos de seguridad perimetral.

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

	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

- La promoción de una cultura organizacional de seguridad de la información, a través de procesos de capacitación y sensibilización dirigidos a servidores públicos, contratistas y terceros que tengan acceso a los activos de información.

El presente plan es de aplicación transversal a todos los procesos y subprocesos de la entidad, y su cumplimiento es de carácter obligatorio para el personal que participe en el manejo, uso, custodia o administración de la información institucional. Su seguimiento y actualización se realizará de manera periódica, de acuerdo con los cambios normativos, tecnológicos y organizacionales que puedan afectar el perfil de riesgo de la entidad.

7. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7.1. Contexto para la Gestión del Riesgo de Seguridad y Privacidad de la Información.

Para la gestión de los riesgos de seguridad y privacidad de la información, la E.S.E. Hospital Regional de Chiquinquirá analiza de manera integral los factores internos y externos que pueden afectar el cumplimiento de sus objetivos estratégicos, misionales, asistenciales, administrativos y de control. Este análisis considera la estructura organizacional, el modelo de operación por procesos, el nivel de cumplimiento de planes, programas y proyectos institucionales, así como la disponibilidad y estado de los recursos físicos, tecnológicos y humanos.

El establecimiento del contexto permite identificar las condiciones bajo las cuales se administran los riesgos, garantizando una adecuada toma de decisiones y la definición de controles proporcionales al nivel de exposición, en concordancia con la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD).

7.2. Criterios de Evaluación del Riesgo:

Para la determinación del nivel de riesgo en materia de seguridad y privacidad de la información, se tienen en cuenta los siguientes criterios:

- Valor estratégico del proceso y de la información para la entidad.
- Nivel de criticidad de los activos de información.

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

CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

- Implicaciones contractuales, legales y regulatorias asociadas.
- Impacto sobre la confidencialidad, integridad y disponibilidad de la información.
- Dependencia de los procesos institucionales respecto de los sistemas de información.

7.3. Criterios de Impacto.

Los criterios de impacto se definen en función del grado de afectación que puede generar un evento de seguridad de la información sobre la entidad, considerando impactos de tipo operativo, asistencial, financiero, legal y reputacional, tales como

- Nivel de clasificación y sensibilidad de los activos de información afectados.
- Existencia de brechas en la seguridad de la información.
- Deterioro o interrupción de la operación institucional y de la prestación de los servicios de salud.
- Pérdida de información crítica y afectación del valor financiero.
- Alteración de planes, cronogramas y compromisos institucionales.
- Daños a la imagen y reputación de la entidad.
- Incumplimiento de requisitos legales y normativos vigentes.

7.4. Criterios de Aceptación del Riesgo

La aceptación del riesgo se define de acuerdo con la tolerancia institucional y la expectativa de duración del riesgo, teniendo en cuenta, entre otros, los siguientes elementos:

- Cumplimiento de los requisitos legales y normativos.
- Capacidad operativa de la entidad para gestionar el riesgo.
- Nivel de madurez tecnológica y disponibilidad de recursos.
- Impacto financiero y sostenibilidad institucional.
- Consideraciones sociales, humanitarias y asistenciales propias del sector salud.

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



CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

7.5. Identificación de Activos de la Información.

Para la identificación de los activos de información, la E.S.E. Hospital Regional de Chiquinquirá, a través del proceso de Tecnologías de la Información y las Comunicaciones (TIC) y en articulación con los líderes de los procesos y subprocesos, realiza la identificación, clasificación y valoración de los activos de información asociados a cada proceso institucional.

Esta actividad permite evaluar la criticidad, sensibilidad e impacto que podría generar la pérdida, alteración o divulgación no autorizada de la información, de conformidad con los lineamientos establecidos en el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y la normatividad vigente aplicable.


Como resultado de este ejercicio, se consolida el inventario de activos de información de los procesos de la entidad, el cual constituye un insumo fundamental para la valoración de riesgos, la definición de controles y la actualización periódica de la matriz de riesgos de seguridad y privacidad de la información.

Ilustración 1 3.3.3. P04 F03 INVENTARIOS DE ACTIVOS DE LA INFORMACIÓN.

INFORMACIÓN DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS													INVENTARIO DE ACTIVOS DE LA INFORMACIÓN											
E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRÁ													E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRÁ											
SECCIÓN DE GESTIÓN DE RECURSOS LOGÍSTICOS													SECCIÓN DE GESTIÓN DE RECURSOS LOGÍSTICOS											
PROCESO	N°	CATEGORÍA / RIESGO	CATEGORÍA / SEÑAL	INFORMACIÓN BÁSICA	DESCRIPCIÓN	TIPO DE ACTIVO	PLURALIDAD O EXCLUSIVIDAD	ESPECIA	ÁREA RESPONSABLE	CARGO RESPONSABLE	MECANISMO DE CONSERVACIÓN	FORMATO	CLASIFICACIÓN DE RIESGO	IMPACTO DE DAÑO	INDICACION	CRITICIDAD	VALOR GENERAL DEL ACTIVO	PROTECCIÓN	PROXIMIDAD	CONTROLES	USUARIOS	FECHA INICIO	FECHA FIN	
Garantía Jurídica y Contractual	1	ACCIONES/CONDICIONALES	Acciones de Faltas	Información	Documento que sirve de base para el seguimiento de los procesos de atención de los usuarios.	Información	Único	Carolina	Oficina Jurídica	Coordinador Oficina Jurídica	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	A ALTA	1 (ALTO)	Documento que contiene decisiones sobre derechos constitucionales y legales.	1	1	ALTA	Oficina Jurídica	Oficina Jurídica	Oficina de Atención al Usuario		
Subproceso Administrativo y Financiero	2	ACTAS	Actas de Comité Administrativo	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité Administrativo, con el fin de garantizar la transparencia y el control de los recursos.	Información	Único	Carolina	Subgerencia Administrativa y Financiera	Subgerente Administrativo y Financiero	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	1 (BAJO)	Los registros a procesos para el apoyo de los usuarios que se generan.	1	3	ALTA	Subgerencia Administrativa y Financiera	Oficina Subgerencia Administrativa y Financiera	Oficina de Atención al Usuario		
Subproceso Científico	3	ACTAS	Actas de Comité Clínico	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité Clínico, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Subgerencia Clínica	Subgerente Clínico	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	1 (BAJO)	Documento de evaluación de los procesos internos que se controlan y mejoran para el funcionamiento de la entidad.	1	3	ALTA	Subgerencia Clínica	Subgerencia Clínica	Subgerencia Clínica		
Subproceso Administrativo y Financiero	4	ACTAS	Actas de Comité de Asesoramiento	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité de Asesoramiento, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Gerencia de Recursos Humanos	Gerente de Recursos Humanos	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	2 (BAJO)	La información contenida en el documento de evaluación de los procesos internos que se controlan y mejoran para el funcionamiento de la entidad.	1	3	ALTA	Subgerencia Administrativa y Financiera	Oficina Subgerencia Administrativa y Financiera	Oficina de Atención al Usuario		
Calidad y Desarrollo de Servicios	5	ACTAS	Actas de Comité de Calidad de Atención en Salud	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité de Calidad de Atención en Salud, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Oficina de Calidad	Coordinador Oficina de Calidad	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	1 (BAJO)	Documento de evaluación de los procesos internos que se controlan y mejoran para el funcionamiento de la entidad.	1	3	ALTA	Subgerencia Clínica	Oficina de Calidad	Subgerencia Clínica		
Garantía Financiera y Contractual	6	ACTAS	Actas de Comité de Control	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité de Control, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Gerencia Financiera y Contractual	Coordinador Financiera y Contractual	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	1 (BAJO)	Los registros a procesos para el apoyo de los usuarios que se generan.	1	3	ALTA	Gerencia Financiera y Contractual	Oficina Subgerencia Administrativa y Financiera	Oficina de Atención al Usuario		
Garantía Jurídica y Contractual	7	ACTAS	Actas de Comité de Contratación	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité de Contratación, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Jurídica	Coordinador Jurídica	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	1 (BAJO)	Documento que registra los temas tratados, decisiones y acuerdos alcanzados por los integrantes de la entidad.	1	3	ALTA	Oficina Jurídica	Oficina Jurídica	Oficina de Atención al Usuario		
Atención de Control Interno	8	ACTAS	Actas de Comité de Control Interno	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité de Control Interno, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Control Interno	Asesor de Control Interno	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	A ALTA	1 (ALTO)	La información que contiene los resultados de los controles internos que se realizan y los planes de acción para mejorarlos.	1	1	ALTA	Asesor de Control Interno	Asesor de Control Interno	Oficina de Atención al Usuario		
Subproceso Administrativo y Financiero	9	ACTAS	Actas de Comité de Convocatoria Laboral	Información	Documento donde se registran los temas tratados y compromisos acordados en el Comité de Convocatoria Laboral, con el fin de garantizar la calidad de los servicios de salud y la atención de los usuarios.	Información	Único	Carolina	Seguridad y Salud en el Trabajo	Coordinador Seguridad y Salud en el Trabajo	Recadigital	PDF	INFORMACIÓN PÚBLICA RESERVADA	M BAJA	2 (BAJO)	La información contenida en el documento de evaluación de los procesos internos que se controlan y mejoran para el funcionamiento de la entidad.	1	3	ALTA	Subgerencia Administrativa y Financiera	Seguridad y Salud en el Trabajo	Seguridad y Salud en el Trabajo		

Fuente: Propia

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

	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

En donde los activos de la información, de cada proceso, se evaluaron en función de la criticidad, integralidad y confidencialidad como lo dispone la guía N° 7 de gestión de riesgos del MINTIC.

Ilustración 2 Criterios de clasificación.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 3 Niveles de clasificación.

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

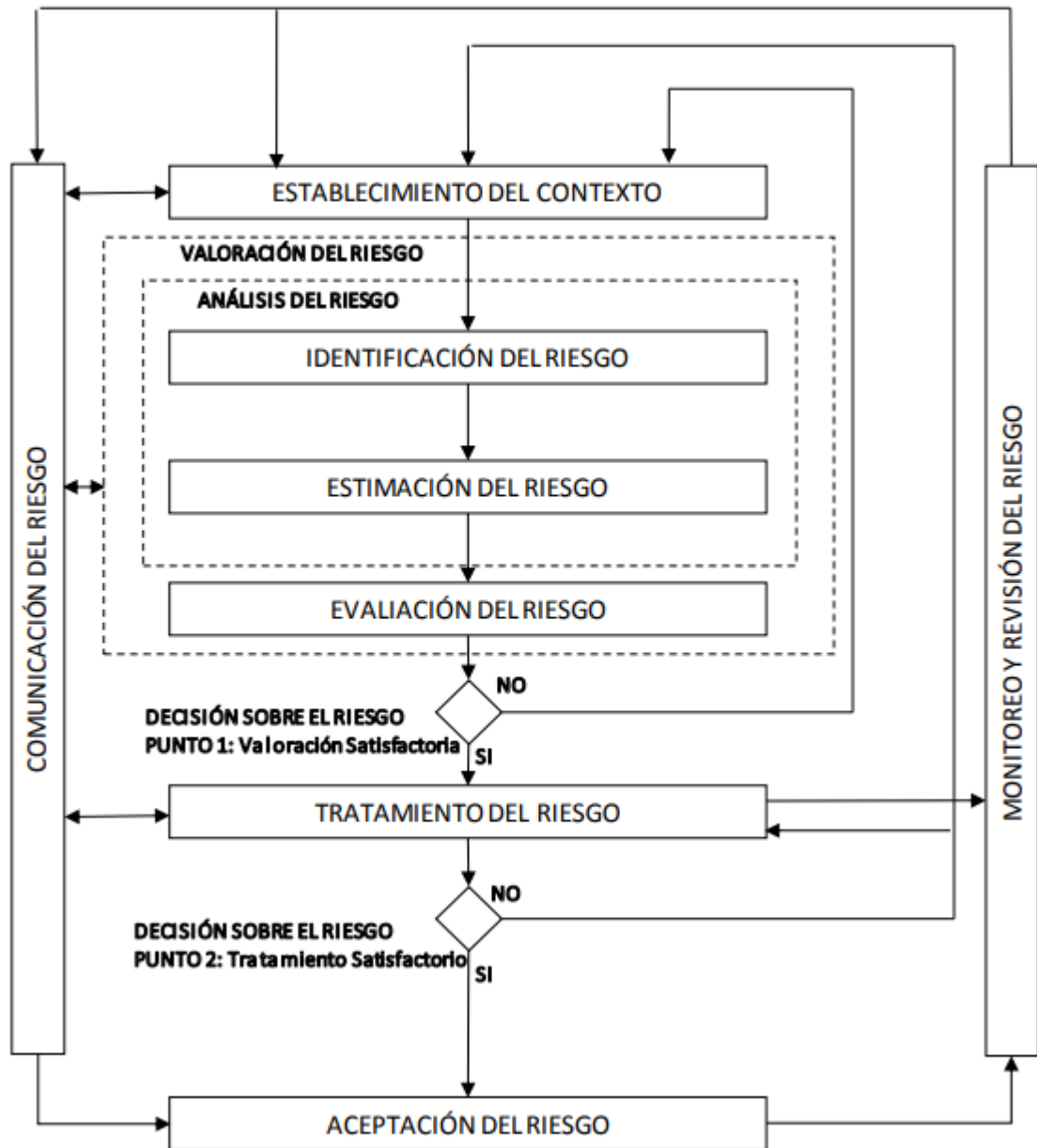


CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN


USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

Ilustración 4 Proceso para la administración del riesgo en seguridad de la información.



Nota: Tomado de la NTC-ISO/IEC 27005

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

	CÓDIGO	3.3.2.D04	<p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

7.6. Riesgos de Tecnologías de la Información y Comunicaciones

7.6.1. Análisis de Riesgos

Mediante la identificación de activos de la información y mediante la tabla de retención documental institucional, se decide agrupar los activos por el tipo de activo en el que actualmente se consideran, de tipo información, según la tabla topología de activos.

- **Tipología de Activos. (MINTIC):** En donde los riesgos a estos activos están directamente en las estaciones de trabajo de cada proceso, y servidores que sirven para contener y brindar el funcionamiento de los sistemas de información, como resultado establecieron dos riesgos en base a las amenazas identificadas.

Ilustración 5 Tipología de Activos. (MINTIC)

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

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



CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

Ilustración 6 Matriz de riesgos TIC.

No. DEL RIESGO	RIESGO	% Probabilidad Inherente	% Impacto Inherente	PROBABILIDAD	IMPACTO	SEVERIDAD (NIVEL DE RIESGO)	% Probabilidad Residual	% Impacto Residual	PROBABILIDAD	IMPACTO	SEVERIDAD (NIVEL DE RIESGO)	¿Requiere Plan de Acción?	Tratamiento	Determine el tratamiento a seguir	Definición del Tratamiento	Descripción de la Acción, basado en el análisis de causas
R1	Posibilidad de efecto dañoso sobre bienes de uso público por no adquisición o renovación oportuna de equipos tecnológicos requeridos para la operación institucional a causa de deficiencias en la planeación tecnológica y presupuestal, incluyendo la ausencia de un plan de renovación y reposición de equipos alineado con el PETI	40%	80%	Baja	Mayor	Alto	40%	80%	Baja	Mayor	Alto	Requiere Plan de Acción	Reducir_Mitigar_Transferir_Evitar	Reducir_Mitigar	Reducir_Mitigar	Formular, aprobar y ejecutar un plan de renovación y reposición de equipos tecnológicos 5%, alineado con el PETI y el presupuesto institucional, que contemple inventario actualizado con el fin de garantizar la disponibilidad oportuna de los equipos requeridos para la operación institucional.
R2	Posibilidad de efecto dañoso sobre el recurso público por pérdida de información sensible, reservada o pública propia del desarrollo de actividad económica de la empresa a causa de vulnerabilidad en la integridad, confidencialidad y disponibilidad de la información y los datos de la ESE	80%	100%	Medio	Catastrófico	Extremo	40%	100%	Baja	Catastrófico	Extremo	Requiere Plan de Acción	Reducir_Mitigar_Transferir_Evitar	Reducir_Mitigar	Reducir_Mitigar	Implementar y fortalecer los controles de seguridad de la información mediante la renovación y gestión de las licencias NAKIVO y la correcta ejecución de las copias de seguridad en la plataforma Proxmox, asegurando la protección de la integridad, confidencialidad y disponibilidad de la información y los datos de la ESE, conforme al SGGSI y al PETI
R3	Posibilidad de efecto dañoso sobre el recurso público por daños de los sistemas de información institucionales a causa de ausencia de mantenimiento preventivo y correctivo al hardware, ataques externos o internos, intrusión a los sistemas de información institucionales, pérdida o no correcta realización del plan de copias de seguridad	80%	80%	Medio	Mayor	Alto	40%	80%	Baja	Mayor	Alto	Requiere Plan de Acción	Reducir_Mitigar_Transferir_Evitar	Reducir_Mitigar	Reducir_Mitigar	Ejecutar y hacer seguimiento al plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica, así como al plan de copias de seguridad de los sistemas de información institucionales, con el fin de garantizar su correcto funcionamiento, disponibilidad y protección.
R4	Posibilidad de pérdida de integridad por confidencialidad y disponibilidad de la información y los datos de la ESE a causa de intrusión a la red interna de la entidad, ataques a los sistemas de información, fraude, hurto de información, sabotaje o accesos no autorizados.	40%	100%	Baja	Catastrófico	Extremo	40%	100%	Baja	Catastrófico	Extremo	Requiere Plan de Acción	Reducir_Mitigar_Transferir_Evitar	Reducir_Mitigar	Reducir_Mitigar	Implementar y fortalecer los controles de seguridad de la información para prevenir intrusiones, ataques, accesos no autorizados y pérdida de información, mediante la ejecución del SGGSI la gestión de la seguridad perimetral, el control de accesos a los sistemas de información, el monitoreo

Fuente: Matriz de Riesgos TIC

Basados a que los riesgos están directamente relacionados con equipos tecnológicos, la probabilidad de fallo, ataque entre otras es muy alta y en caso de materializarse el impacto podría llegar a ser catastrófico.

Ilustración 7 Matriz de calor inherente

No. DEL RIESGO	RIESGO	CALIFICACIÓN RIESGO INHERENTE		
		PROBABILIDAD	IMPACTO	SEVERIDAD (NIVEL DE RIESGO)
R1	Posibilidad de efecto dañoso sobre bienes de uso público por no adquisición o renovación oportuna de equipos tecnológicos requeridos para la operación institucional a causa de deficiencias en la planeación tecnológica y presupuestal, incluyendo la ausencia de un plan de renovación y reposición de equipos alineado con el PETI	Baja	Mayor	Alto
R2	Posibilidad de efecto dañoso sobre el recurso público por pérdida de información sensible, reservada o pública propia del desarrollo de actividad económica de la empresa a causa de vulnerabilidad en la integridad, confidencialidad y disponibilidad de la información y los datos de la ESE	Medio	Catastrófico	Extremo
R3	Posibilidad de efecto dañoso sobre el recurso público por daños de los sistemas de información institucionales a causa de ausencia de mantenimiento preventivo y correctivo al hardware, ataques externos o internos, intrusión a los sistemas de información institucionales, pérdida o no correcta realización del plan de copias de seguridad	Medio	Mayor	Alto
R4	Posibilidad de pérdida de integridad por confidencialidad y disponibilidad de la información y los datos de la ESE a causa de intrusión a la red interna de la entidad, ataques a los sistemas de información, fraude, hurto de información, sabotaje o accesos no autorizados.	Baja	Catastrófico	Extremo
R5	Posibilidad de pérdida de confidencialidad por desconocimiento del personal sobre políticas, procedimientos y buenas prácticas de seguridad digital y respuesta a incidentes a causa de debilidad de un programa formal y periódico de sensibilización, capacitación en seguridad de la información, alineado con el SGGSI y el modelo de seguridad digital institucional	Medio	Mayor	Alto

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



E.S.E. HOSPITAL REGIONAL DE
CHIQUINQUIRÁ

CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ

Fuente: Matriz de Riesgos TIC

Ilustración 8 Mapa de Calor Residual

MAPA DE CALOR RIESGO RESIDUAL						
		Impacto				
		Leve	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Muy Alta					
	Alta					
	Media					
	Baja				R1 R3 R5	R2 R4
	Muy Baja					

Fuente: Matriz de Riesgos TIC

7.7. Controles


7.7.1. Determinación de Controles.

Debido al resultado del análisis y evaluación de los riesgos, desde el proceso de tecnologías de la información se proponen controles para mitigar y/o compartir el impacto y la probabilidad de materialización.

- **Control 1. Fortalecimiento de la capacidad instalada tecnologías de la información.**

Actividad y/o herramienta.

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

	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

Gestionar la adquisición de equipos y licencias tecnológicas para evitar la materialización del riesgo.

La gestión oportuna de la adquisición de equipos y licencias tecnológicas es fundamental para garantizar la disponibilidad, estabilidad y seguridad de la infraestructura tecnológica institucional. La falta de equipos adecuados o de licencias vigentes puede generar fallas operativas, indisponibilidad de los sistemas de información, lo que representa un riesgo de afectación al recurso público.

Este control permite prevenir la obsolescencia tecnológica, asegurar la continuidad de los procesos institucionales y reducir la probabilidad de materialización del riesgo identificado, en concordancia con el PETI y los lineamientos de Control Interno.

Responsables.

- El Líder de Tecnologías de la Información
- Gestión financiera y oportunidad contractual de los suministros e insumos tecnológicos, contrato de mantenimiento - Subgerencia Administrativa y Financiera

➤ **Control 2. Mantenimiento preventivo y correctivo.**

Actividad y/o herramienta.

Ejecutará, junto con su equipo de trabajo, el plan de mantenimiento correctivo y preventivo, así como el plan de copias de seguridad proyectados para la vigencia.

El mantenimiento a los equipos y periféricos de informática y comunicaciones en la entidad, mitiga la posibilidad de daño mecánico y eléctrico, a su vez al realizar mantenimiento al software, mejora el rendimiento en la protección de la información.

Responsables.

- Ejecución del mantenimiento - Proceso TIC.
- Gestión financiera y oportunidad contractual de los suministros e insumos tecnológicos, contrato de mantenimiento - Subgerencia Administrativa y Financiera

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

CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

**PLAN DE TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ****➤ Control 3. Seguridad perimetral****Actividad y/o herramienta.**

Gestionará la adquisición de equipos, las licencias para la seguridad perimetral

La gestión oportuna de la adquisición de equipos y licencias para la seguridad perimetral permite fortalecer la protección de la infraestructura tecnológica y de los sistemas de información institucionales, reduciendo la probabilidad de intrusiones, ataques externos o accesos no autorizados.

Responsables.

- El Líder de Tecnologías de la Información
- Gestión financiera y oportunidad contractual, contrato de - Subgerencia Administrativa y Financiera

➤ Control 4. Planes de actualización, parches de servidores.**Actividad y/o herramienta.**

Ejecutará planes de actualización, parches de servidores, aplicaciones y equipos de red.

La ejecución de planes de actualización, aplicación de parches en servidores, aplicaciones y equipos de red es necesaria para corregir vulnerabilidades, prevenir fallas de seguridad y reducir el riesgo de accesos no autorizados o ataques informáticos. Este control permite mantener los sistemas de información actualizados y protegidos, garantizar la confidencialidad, integridad y disponibilidad de la información, y salvaguardar el recurso público.

Responsables.

- El Líder de Tecnologías de la Información
- Gestión financiera y oportunidad contractual, contrato de - Subgerencia Administrativa y Financiera

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

CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

**PLAN DE TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN****USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ**➤ **Control 5. Respaldo de la información.****Actividad y/o herramienta.**

Administración del dispositivo de almacenamiento NAS, conectado en red y ejecución del cronograma de copias de seguridad.

El dispositivo permite una gestión de almacenamiento centralizado y protegido contra pérdidas de información gracias a su tecnología y configuración; mediante la herramienta permitirá ejecutar el plan de copias de seguridad cuyo objetivo es respaldar la información de manera semestral o anual de acuerdo al valor estratégico de cada proceso.

Responsables.

- Implementación de herramientas y dispositivos para la ejecución del cronograma de copias de seguridad - Proceso TIC.
- Compromiso, consolidación y organización de la información - Líderes y coordinadores de cada proceso y subproceso.

➤ **Control 6. Capacitación y sensibilización seguridad de la información.****Actividad y/o herramienta.**

Capacitar sobre seguridad digital para todo el personal, enfocándose en las mejores prácticas para proteger la información y los sistemas.


Con la capacitación al personal de la entidad, se mitiga la probabilidad de pérdida de información por mala manipulación de los equipos, documentos, ataques dirigidos al usuario (phishing), a su vez sensibilizar acerca de las políticas de seguridad que rigen la institución.

Responsables.

- Gestión capacitación - Proceso TIC.
- Compromiso por parte de la alta dirección en el apoyo y socialización en las áreas administrativas y asistenciales para asistencia.
- Compromiso de adopción de políticas y guías para la seguridad digital es todo el personal de la E.S.E Hospital Regional Chiquinquirá.

En donde la implementación y ejecución de actividades y controles se espera atacar proporcionalmente el impacto y la probabilidad.

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

	CÓDIGO	3.3.2.D04	<p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

8. Análisis Integral DOFA

FORTALEZAS (ANÁLISIS INTERNO)		DEBILIDADES (ANÁLISIS INTERNO)	
1	Existencia del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información actualizado	1	Dependencia de la disponibilidad presupuestal para la adquisición oportuna de equipos, licencias y soluciones de seguridad.
2	Identificación, clasificación y valoración de los activos de información conforme a criterios de confidencialidad, integridad y disponibilidad.	2	Limitaciones en la capacidad instalada de infraestructura tecnológica frente al crecimiento de los servicios y de la información
3	Proceso de Tecnologías de la Información y las Comunicaciones formalmente establecido y articulado con los demás procesos institucionales	3	Riesgos asociados a la obsolescencia tecnológica de algunos equipos y sistemas
4	Compromiso de la alta dirección en el fortalecimiento de la seguridad de la información.	4	Brechas en el nivel de conocimiento y apropiación de las políticas de seguridad de la información por parte del personal.
OPORTUNIDADES (ANÁLISIS EXTERNO)		AMENAZAS (ANÁLISIS EXTERNO)	
1	Lineamientos, guías y herramientas emitidas por el MINTIC y el DAFP para el fortalecimiento de la seguridad digital en entidades públicas.	1	Riesgo de pérdida, alteración o divulgación no autorizada de información sensible y datos personales.
2	Avances tecnológicos en soluciones de ciberseguridad, respaldo, almacenamiento y protección perimetra	2	Fallas en la infraestructura tecnológica que puedan afectar la disponibilidad de los sistemas de información críticos.
3	Posibilidad de fortalecer la interoperabilidad de los sistemas de información en salud bajo estándares de seguridad	3	Cambios constantes en la normatividad y exigencias regulatorias en materia de seguridad de la información.
4	Fortalecimiento de la cultura de gestión del riesgo y control interno en la entidad.	4	Dependencia de proveedores externos para servicios tecnológicos críticos.

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

CÓDIGO	3.3.2.D04
VERSIÓN	08
FECHA	Ene. 30 de 2026
TIPO	PLAN
PROCESO	GESTION DE RECURSOS LOGISTICOS

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

USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ


9. Recursos Necesarios y Presupuesto Estimado

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

10. Recomendaciones

- Fortalecer la gobernanza de la seguridad y privacidad de la información, asegurando la articulación entre TIC, Planeación, Control Interno y la Alta Dirección.
- Mantener actualizado el inventario y la clasificación de los activos de información, conforme a los cambios tecnológicos, operativos y normativos.
- Priorizar la asignación de recursos para la renovación, mantenimiento y seguridad de la infraestructura tecnológica y los sistemas de información críticos.
- Consolidar la implementación de controles técnicos de seguridad, incluyendo actualización de sistemas, seguridad perimetral y respaldo de la información.
- Garantizar la ejecución, verificación y prueba periódica de las copias de seguridad, asegurando la disponibilidad y recuperación oportuna de la información.

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


	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

- Desarrollar programas de capacitación y sensibilización en seguridad y privacidad de la información para todo el personal.
- Realizar seguimiento a los riesgos residuales y a la efectividad de los controles implementados, promoviendo la mejora continua del plan.

11. Documentos Relacionados del Sistema Integrado de Gestión


CODIGO	DESCRIPCION
3.3.2.D01	PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION
3.3.2.D02	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
3.3.2.D02.F01	REGISTRO DE NACIMIENTOS ATENDIDOS ESE HRC
3.3.2.D02 F02	COMPROMISO DE SEGURIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD DE LA INFORMACION
3.3.2.D03	PLAN DE DATOS ABIERTOS
3.3.2.D03 F01	REGISTRO DE NACIMIENTOS ATENDIDOS EN LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D03 F02	REGISTRO DE DEFUNCIONES ATENDIDOS EN LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D03 F03	REGISTRO BASE DE DATOS SIVIGILA ESE HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D03 F04	REGISTRO BASES DE DATOS MORBILIDAD ESE HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D04	PLAN DE TRATAMIENTO DE RIESTGOS DE SEGURIDAD DE LA INFORMACION
3.3.2.D05	MODELO DE ARQUITECTURA EMPRESARIAL
3.3.2.D06	MODELO DE GESTION Y GOBIERNO DE TI
3.3.2.D07	MODELO DE GESTION DE PROYECTOS DE TI
3.3.2.P01	MANTENIMIENTO PREVENTIVO A EQUIPOS TECNOLOGICOS
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.P01 F03	LISTA DE VERIFICACION MANTENIMIENTO PREVENTIVO
3.3.2.P02	MANTENIMIENTO CORRECTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA
3.3.2.P02 F01	MANTENIMIENTO CORRECTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA
3.3.2.P03	COPIA DE SEGURIDAD DEL SISTEMA DGH

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

	CÓDIGO	3.3.2.D04	<p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

3.3.2.P04	COPIA DE SEGURIDAD DEL SISTEMA SAIH
3.3.2.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.P07 F01	RECEPCIÓN DE SERVICIO DE SISTEMAS
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
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.P19 F01	REGISTRO DE VARIACIONES EN LOS SISTEMAS DE INFORMACION
3.3.2.P20	SOLICITUD DE BASES DE DATOS DE LOS SISTEMAS DE INFORMACION
3.3.2.R01	ADMINISTRACION Y CONTROL DE LICENCIAS
3.3.2.R02	PRUEBAS DE EFECTIVIDAD
3.3.2.R03	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION
3.3.2.R04	SEGURIDAD DEL RECURSO HUMANO
3.3.2.R05	GESTION DE ACTIVOS
3.3.2.R06	CONTROL DE ACCESO
3.3.2.R07	CONTROLES CRIPTOGRAFICOS PARA LA PROTECCION DE LA INFORMACION
3.3.2.R08	SEGURIDAD FISICA Y DEL ENTORNO PARA LA PROTECCION DE LA INFORMACION
3.3.2.R09	SEGURIDAD DE LAS OPERACIONES
3.3.2.R10	SEGURIDAD DE LAS COMUNICACIONES DE TI
3.3.2.R11	ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
3.3.2.R12	RELACIONES CON LOS PROVEEDORES
3.3.2.R13	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION
3.3.2.R14	GESTION DE CONTINUIDAD DEL NEGOCIO
3.3.2.R15	CUMPLIMIENTO DE LOS REQUISITOS LEGALES DE TI
3.3.2.R16	ROLES Y RESPONSABILIDADES DE TI
3.3.2.R17	ROLES Y RESPONSABILIDADES DE TI

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

	CÓDIGO	3.3.2.D04	<p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

3.3.2.R18	DATOS MAESTROS, MINERIA DE DATOS Y EXPLOTACION DE DATOS
3.3.2.R19	COMUNICACIONES, CAPACITACION Y SENSIBILIZACION SOBRE LA SEGURIDAD DE LA INFORMACION
3.3.2.R20	GESTION DE LA TECNOLOGIA TIC
3.3.2 T01	TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES
3.3.2. T02	Caracterización Subproceso Tecnologías de Información y las Comunicaciones


12. Indicadores de Éxito

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

13. Actividades y Cronograma

Nº	ASPECTOS/CRITERIOS	ACTIVIDAD	META	SOPORTE	RESPONSABLE	FECHA PROGRAMADA
1	Tecnologías de la Información y la comunicación	Realizar seguimiento de los controles de la matriz de riesgos institucional de acuerdo al nivel de aceptación, mitigación o consecución del riesgo, según sea el caso	100%	Informe de resultados	Líder de Tecnologías de la Información	30/04/2026 31/08/2026 31/12/2026
2	Tecnologías de la Información y la comunicación	Informe de seguimiento a la matriz de riesgos	100%	Informe de resultados	Informe de resultados	31/12/2026

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

	CÓDIGO	3.3.2.D04	<p align="center">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			




14. Seguimiento y Evaluación


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

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 https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf
2	Política de Gobierno Digital. (s/f). Gov.co. Recuperado el 29 de enero de 2025, de https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/
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 https://mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_2024_20240125.pdf


16. Revisión y aprobación

ÍTEM	ELABORÓ	COORDINADOR	REVISÓ	APROBÓ
Firma				
Nombre	Jonathan García	Jonathan García	Luber Ney Murcia	Juliana del Pilar Cortázar Murillo
Cargo	Líder Tecnologías de la Información	Líder Tecnologías de la Información	Coordinador de Planeación Estratégica	Gerente
Fecha	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.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			

17. 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	Roosbelth 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.	7	Jonathan García Líder Tecnologías de la Información	Juliana del Pilar Cortázar Murillo Gerente
Ene. 30 de 2026	7	Actualización anual	En todo el documento teniendo en cuenta las nuevas metas del área.	8	Jonathan García Líder Tecnologías de la Información	Juliana del Pilar Cortázar Murillo Gerente

SISTEMA OBLIGATORIO DE GARANTÍA DE LA CALIDAD DE ATENCIÓN EN SALUD DEL SGSSS			
	CÓDIGO	3.3.2.D04	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
	VERSIÓN	08	
	FECHA	Ene. 30 de 2026	
	TIPO	PLAN	
	PROCESO	GESTION DE RECURSOS LOGISTICOS	
USO DE LA ESE HOSPITAL REGIONAL DE CHIQUINQUIRÁ			