E.S.E. HOSPITAL REGIONAL DE DUITAMA

Plan de servicio: Plan De Tratamiento De Riesgos De Seguridad De La Información

ENERO 2026

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

TABLA DE CONTENIDO

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

1. Introducción

Este documento define la estrategia para la gestión y tratamiento de los riesgos de seguridad y privacidad de la información, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI).

2. Objetivo

Administrar los riesgos de seguridad mediante su identificación, análisis, control y evaluación, garantizando la confidencialidad, integridad y disponibilidad de los activos de información

3. Responsable

Líder Tecnología De La Información (Tecnologías de la Información)

4. Alcance

Aplica a todos los activos de información e infraestructura crítica de la E.S.E. Hospital Regional de Duitama y sus sedes anexas.

Se han priorizado seis (6) riesgos clave que podrían afectar la prestación de servicios de salud y los procesos administrativos:

Cód.	Riesgo	Probabilidad	Impacto	Nivel de Riesgo
R-T102	Encriptación o secuestro de información (Ransomware)	Media (60%)	Catastrófico (100%)	EXTREMO
R-T105	Incidentes en los centros de datos de la entidad	Baja (40%)	Mayor (80%)	ALTO
R-T101	Interrupción de servicios de salud/administrativos	Media (60%)	Moderado (60%)	Moderado
R-T104	Fallas en servicios tecnológicos (Internet, Red, Voz)	Media (60%)	Moderado (60%)	Moderado
R-T106	Alteración de información sensible por terceros	Baja (40%)	Moderado (60%)	Moderado
R-T103	Uso inadecuado de software e información digital	Baja (40%)	Menor (40%)	Moderado

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

Para cada uno de estos riesgos, se establecen controles y tratamientos correctivos o preventivos, los cuales permiten monitorear, dar seguimiento y evaluar su mitigación progresiva. Esto da lugar a un plan de implementación que será ejecutado durante la vigencia 2026.

Considerando los objetivos institucionales y la necesidad de reducir el impacto de los riesgos, para 2026 se ha priorizado la intervención del riesgo de mayor nivel: la posible encriptación o secuestro de la información digital en las bases de datos de los sistemas de información y archivos de los equipos de cómputo.

5. Responsables

ÁREA O ROL INSTITUCIONAL	RESPONSABILIDADES
Directivos de la Entidad	Encargados de la aprobación de los proyectos de inversión en temas de seguridad y privacidad de la información.
Control Interno, Planeación Institucional y Gestión de Calidad.	Responsables de auditorías, control y seguimiento al tratamiento de riesgos de seguridad de la información.
Líder de Tecnologías de la Información	Responsables del tratamiento de los riesgos de seguridad de la información.
Responsable de la seguridad Institucional	
Equipo de Tecnologías de la Información	
Líderes y Coordinadores institucionales	

6. Marco Legal y/o Teórico

Políticas técnicas de seguridad de la Información Función Pública, 2020: La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades.

Decreto 103 de 2015, 2019: Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.

Decreto 1494 de 2015, 2019: Por el cual se reglamenta parcialmente la Ley 171de 2014 y se dictan otras disposiciones.

Decreto 1008, 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

Ley 1712 de 2014, 2018: Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

Decreto 2573 de 2014, 2018: Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.

Decreto 1377 de 2013, 2018: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

Decreto 2609 de 2012, 2017: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley estatutaria 1581 de 2012, 2017: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
Ley 1474 de 2011, 2017: Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Ley 527 de 1999, 2015: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Norma técnica colombiana NTC - ISO/IEC 27001, 2013: Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.
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.

7. Diagnostico y/o situación actual

En el modelo de seguridad y privacidad de la información, el la FASE 1: Diagnostico, se tiene el análisis de la situación actual de la entidad, con la metodología para la identificación de los activos de la información y la infraestructura critica. El Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información en un producto que enfatiza su contenido para el control y tratamiento de los riesgos.

8. Definiciones

Activo: Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización - Servicios web -Redes - Información física o digital -Tecnologías de información TI - Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.
Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
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).
Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.
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).

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

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: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
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.
Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
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.

9. Recursos, Materiales, Insumos y Equipos

El presente documento es un producto del programa institucional "Modelo de Seguridad y Privacidad de la Información". Este documento se utiliza como insumo para ver el estado actual de la entidad en relación a seguridad y privacidad de la información y de esa forma determinar los riesgos inherentes a Seguridad Digital.

10. Desarrollo

10.1 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SITUACIÓN ACTUAL

En el modelo de seguridad y privacidad de la información, el la FASE 1: Diagnostico, se tiene el análisis de la situación actual de la entidad, con la metodología para la identificación de los activos de la información y la infraestructura critica. El Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información en un producto que enfatiza su contenido para el control y tratamiento de los riesgos.

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

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

La entidad, integrando el Modelo de Seguridad y Privacidad de la Información (MSPI) con el objetivo de implementar un Sistema de Gestión de Seguridad de la Información, gestiona este documento alineado con la fase de implementación del MSPI.

10.3 RIESGOS

A través del software institucional Almera, en el cual se gestionaron los riesgos de seguridad y privacidad de la información, se puede obtener un análisis resumido de los seis (6) riesgos relacionados a los activos de la información y a la infraestructura critica, los cuales son:

Cód.	Riesgo	Probabilidad	Impacto	Nivel de Riesgo
R-T102	Encriptación o secuestro de información (Ransomware)	Media (60%)	Catastrófico (100%)	EXTREMO
R-T105	Incidentes en los centros de datos de la entidad	Baja (40%)	Mayor (80%)	ALTO
R-T101	Interrupción de servicios de salud/administrativos	Media (60%)	Moderado (60%)	Moderado
R-T104	Fallas en servicios tecnológicos (Internet, Red, Voz)	Media (60%)	Moderado (60%)	Moderado
R-T106	Alteración de información sensible por terceros	Baja (40%)	Moderado (60%)	Moderado
R-T103	Uso inadecuado de software e información digital	Baja (40%)	Menor (40%)	Moderado

A. Controles y Tratamiento (Matriz de Control 2026)

Para mitigar estos riesgos, se mantienen y refuerzan los siguientes controles:

- Infraestructura: Configuración de red de datos en anillo redundante con segmentación por VLAN para mejorar el tráfico y la seguridad.
- Mantenimiento: Ejecución de mantenimientos preventivos programados y reposición de hardware obsoleto para evitar fallas críticas.
- Ciberseguridad: Implementación de seguridad perimetral empresarial gestionada por expertos externos para combatir ataques cibernéticos.
- Capacitación: Programas de inducción y reinducción para usuarios finales sobre el uso correcto de los sistemas.
- Legal: Inclusión de cláusulas de confidencialidad y privacidad en contratos de talento humano y proveedores.

B. Controles y Tratamiento (Matriz de Control 2026)

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

Para mitigar estos riesgos, se mantienen y refuerzan los siguientes controles:

- Infraestructura: Configuración de red de datos en anillo redundante con segmentación por VLAN para mejorar el tráfico y la seguridad.
- Mantenimiento: Ejecución de mantenimientos preventivos programados y reposición de hardware obsoleto para evitar fallas críticas.
- Ciberseguridad: Implementación de seguridad perimetral empresarial gestionada por expertos externos para combatir ataques cibernéticos.
- Capacitación: Programas de inducción y reinducción para usuarios finales sobre el uso correcto de los sistemas.
- Legal: Inclusión de cláusulas de confidencialidad y privacidad en contratos de talento humano y proveedores.

10.4 Plan de Implementación Prioritario - Vigencia 2026

Dada la criticidad, para el año 2026 se ha priorizado la intervención del riesgo R-T102 (Secuestro de información).

Actividad: Implementar una solución profesional de seguridad perimetral (basada en el cuadrante mágico de Gartner), con gestión especializada de políticas de seguridad y conexión segura entre sedes.

- Responsable: Líder de Tecnologías de la Información.
- Fecha de Inicio: 01 de enero de 2026.
- Fecha de Finalización: 30 de junio de 2026.

10.5 Monitoreo y Evaluación 2026

El seguimiento se realizará de forma sistemática por la Oficina de Control Interno:

1. Primer Seguimiento: Corte al 30 de mayo de 2026.
2. Segundo Seguimiento: Corte al 31 de agosto de 2026.
3. Tercer Seguimiento: Corte al 31 de diciembre de 2026.

Los resultados y la eficacia de las acciones de mejora serán publicados en la página web institucional para consulta ciudadana.

11. PLAN DE IMPLEMENTACIÓN

Teniendo en cuenta el objetivo de la entidad, para disminuir la probabilidad o mitigar el impacto de los riesgos, para la vigencia 2024, de opta por intervenir el riesgo con mayor nivel de riesgo, el cual pertenece a:

Código	Nombre	Probabilidad (Riesgo Inherente)	Impacto (Riesgo Inherente)	Nivel de Riesgo (Riesgo Inherente)

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

R-TI02	Posibilidad de encriptación o secuestro de la información digital de las bases de datos de los sistemas de información y archivos de los equipos de cómputo.	Media (60%)	Catastrófico (100%)	Extremo

Que genera una actividad correctiva o acción de mejora relacionada a:

Oportunidad de mejora identificada	**Tipo de acción a desarrollar**	**Plan de acción**			
	Acción preventiva/ correctiva/ mejora.	**Actividad**	**Responsable**	**Fecha inicio**	**Fecha final**
Implementar una solución profesional de seguridad perimetral.	Acción correctiva.	Implementar una solución profesional de seguridad perimetral, basada por el cuadrante mágico de Gartner, cuya administración sea Realizada por una empresa con experiencia en ciberseguridad y se garantice la gestión de politicas de seguridad y correcto funcionamiento de los equipos entregados. Soporte: Informe de implementación de una solución de seguridad perimetral y	Líder de Tecnologías de la Información.	01 Ene. 2026	30 Jun 2026

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

		conexión entre sedes anexas.			

12. CAPACITACIÓN

La socialización del Plan de Tratamiento de Riesgos de Seguridad de la Información, se realizará principalmente en las reuniones directivas, en las cuales, el personal directivo de la entidad, líderes y coordinadores tiene una participación directa con la adopción de las políticas de seguridad de la información y de esta forma, hacerlos participes de los riesgos institucionales en relación a Seguridad Digital.
Los colaboradores, contratistas y terceros, tendrán una ayuda audiovisual para conocer el documento y los riesgos, ya que una buena gestión del conocimiento, permite mitigar la ocasión de incidentes de seguridad.
Adicionalmente en los procesos de capacitación institucional, será informado al personal los temas de seguridad y privacidad de la información y riesgos de seguridad Digital.

13. Bibliografía

Dirección de Gestión y Desempeño Institucional diciembre de 2020. (s.f.). Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública, versión 5.

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Guia de gestión de Riesgos Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y Comunicaciones. (OCTUBRE 2021). Documento Maestro del Modelo de Seguridad y Privacidad de la Información. Modelo de Seguridad y Privacidad de la Información.

14. ANEXOS.

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad

Revisión y Aprobación		
Elaborado/Modificado por:	**Cargo:**	**Fecha:**
Luis Gabriel Ramírez Núñez	Líder de Gestión Tecnologías de la Información	7/01/2026
Revisado por:	**Cargo:**	**Fecha:**
Nicolás Daniel Arévalo Rodríguez Iris Adriana Mojica Carvajal	Líder de Planeación y del Sistema Integrado de Gestión de Riesgos Líder de Calidad y Acreditación	28/01/2026
Aprobado por:	**Cargo:**	**Fecha:**
Jairo Mauricio Santoyo Gutiérrez	Gerente	29/01/2026

Este documento es propiedad de la Empresa Social del Estado Hospital Regional de Duitama.
Su reproducción es estará dada por el líder del proceso de gestión de calidad