SUBDIRECCIÓN ADMINISTRATIVA
UNIDAD DE INFORMÁTICA
HOSPITAL MILITAR CENTRAL - HOMIL
CÓDIGO: GT-UNIN-PL-05, ,
VERSIÓN: 01
FECHA DE EMISIÓN: 21-01-2026

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Plan de Tratamiento de Riesgos de Seguridad de la Información 2026

Ingeniero José Miguel Cortes García
Subdirector del Sector Defensa
Subdirección Administrativa (E)
Hospital Militar Central

Teniente Coronel Eduardo Enrique Mendoza Palacio
Jefe de Unidad Seguridad y Defensa
Unidad de Informática
Hospital Militar Central

Capitán Luis Fernando Sierra Joya
Oficial de Seguridad de la información
Hospital Militar Central

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Hospital Militar Central – HOMIL, mediante la directiva permanente N° 002 del 15 de junio de 2021 "Lineamientos Para la Implementación de la Política de Gobierno Digital en el Hospital Militar Central" adoptó lo contenido en la resolución 500 de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital. Asimismo, establece las directrices y estándares para la estrategia de seguridad digital.

Por lo anterior y teniendo en cuenta que el Modelo de Seguridad y Privacidad de la Información – MSPI indica que las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI, identificar los dueños de los riesgos, definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia, determinar el apetito de riesgos definido por la Entidad, establecer criterios de aceptación de los riesgos, aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance, determinar los niveles de riesgo, realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral y priorización de los riesgos analizados para su tratamiento; la entidad adoptó la Guía para la gestión de riesgos de seguridad de la información (Anexo 4. DAFP) y la incluyó dentro de la Política de Operación para la Administración del riesgo en Hospital Militar Central en el numeral 8.7 – Lineamientos riesgos de Seguridad de la Información

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer y aplicar un marco integral para identificar, evaluar y tratar los riesgos de seguridad y privacidad de la información en el Hospital Militar Central, considerando vulnerabilidades de los activos de información, obsolescencia tecnológica y métodos y técnicas utilizados por ciberdelincuentes, con el fin de proteger la confidencialidad, integridad, disponibilidad, privacidad y autenticidad de la información, garantizando el cumplimiento de las normas, leyes y regulaciones vigentes en materia de protección de datos y seguridad de la información.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar, evaluar y gestionar los riesgos de seguridad de la información, asegurando la confidencialidad, integridad, disponibilidad y autenticidad de los activos de información.
- Implementar los controles del Sistema de Gestión de Seguridad de la Información (SGSI) necesarios para cumplir con los requisitos del MSPI, mitigar los riesgos sobre los activos de información y proteger la información crítica de nuevas amenazas cibernéticas.

3. ALCANCE

El presente plan de tratamiento de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información identificados en el Hospital Militar Central en cada uno de los procesos con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de

Gobierno Digital" para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

4. JUSTIFICACIÓN

La elaboración del presente Plan de Tratamiento de Riesgos de Seguridad de la información se fundamenta en la necesidad de alinear las Tecnologías de la Información y las Comunicaciones (TIC) con el direccionamiento estratégico, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el enfoque de gestión de riesgos definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este plan hace parte del Sistema de Gestión de Seguridad de la Información (SGSI) y permite identificar, evaluar y tratar de manera sistemática los riesgos de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los activos de información. Asimismo, contribuye a la optimización de los procesos, fortalecimiento de la seguridad de la información y al cumplimiento de los requisitos legales y normativos aplicables.

5. MARCO LEGAL

Al HOMIL para efectos de este Plan de Tratamientos de Riesgos de Seguridad de la Información lo rigen las siguientes normas:

Marco Normativo	Descripción
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones
Ley 1955 del 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Marco Normativo	Descripción
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	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.
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS" "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".
Ley 962 de 2005	El artículo 14 dice lo siguiente: "Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá´ al usuario. Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite".
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	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
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 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.

Marco Normativo	Descripción
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
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 2106 del 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
Resolución 463 de 2022	Por la cual se define el uso de tecnologías en la nube para el sector defensa y se dictan otras disposiciones.
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.

Marco Normativo	Descripción
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

6. ALINEACIÓN ESTRATÉGICA

Los siguientes son los motivadores estratégicos a nivel nación, a nivel territorio, a nivel entidad y los lineamientos y políticas que dan línea en la orientación y alineación la Estrategia de Tecnologías de la Información del Hospital Militar Central:

Ilustración 1. Motivadores Estratégicos – MINTIC

Motivador	Fuente
Estrategia Nacional	Política de Gobierno Digital Política de Seguridad Digital Marco de interoperabilidad del Estado Colombiano Marco de transformación digital del Estado Colombiano Plan Nacional de Desarrollo
Estrategia Sectorial	Plan Estratégico de Tecnologías de la Información del Ministerio de Defensa Nacional Plan de Interoperabilidad del Ministerio de Salud
Estrategia Institucional	Plan Estratégico Institucional
Lineamientos y Políticas	Plan de Transformación Digital - HOMIL Política de Gobierno Digital - HOMIL

Motivador	Fuente
	Modelo Integrado de Planeación y Gestión

Tabla 2. Motivadores Estratégicos - Tomado de MINTIC

6.1 POLÍTICAS, PLANES Y PROGRAMAS INTERNACIONALES, NACIONALES Y SECTORIALES

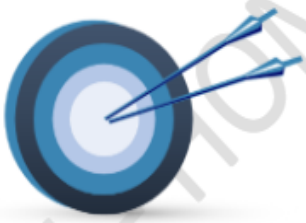
Lo contenido en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2023-2026; en el numeral 9 "Estrategia de TI" y numeral 11.9 HOSPITAL MILITAR CENTRAL. El Plan Estratégico de Tecnologías de la Información del Hospital Militar Central está alineado con:

- La Política de Gobierno Digital busca fortalecer la relación entre los ciudadanos y el Estado mediante el aprovechamiento de las TIC.
- El Plan Nacional de Desarrollo tiene como objetivo democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en el país, promoviendo un entorno digital seguro para generar confianza en el uso y apropiación de las TIC.
- El Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2023-2026 establece la estrategia de TI y las acciones específicas para el Hospital Militar Central.

6.2 MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG

El Plan Estratégico de Tecnologías de la Información (PETI) se encuentra alineado al Marco General del Modelo Integrado de Planeación y Gestión con lo relacionado en las políticas de gestión y desempeño institucional 11 (Gobierno Digital) y 12 (Seguridad Digital).

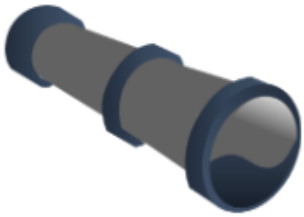
6.3 PLAN ESTRATÉGICO INSTITUCIONAL



MISIÓN

Prestar servicios integrales especializados a los usuarios del Subsistema de Salud de las Fuerzas Militares centrados en el paciente y su familia y gestionar conocimiento a través de la academia y la investigación.

HOSPITAL MILITAR CENTRAL



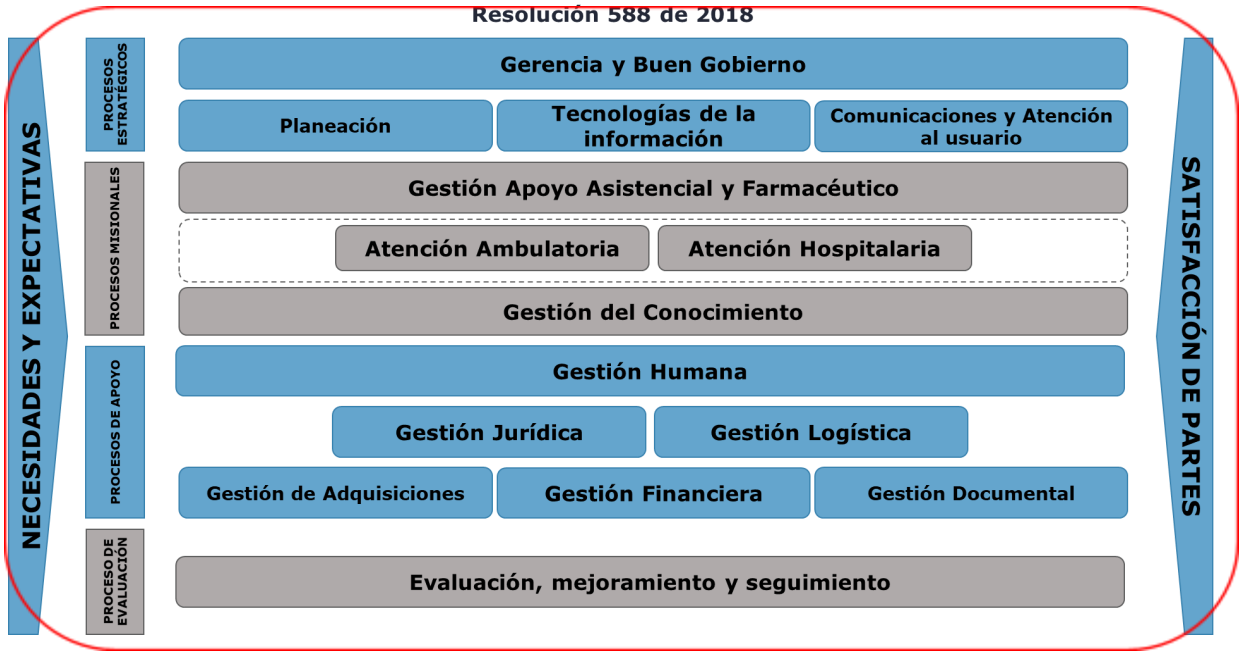
VISIÓN

El Hospital Militar Central continuará siendo la reserva estratégica de la nación en servicios integrales de salud y generación del conocimiento.

Con el ánimo de asegurar el Gobierno Digital en el Hospital Militar Central, la Unidad de Informática en apoyo a los procesos del Hospital Militar Central genera el proceso de transformación e implementación del Plan Estratégico de Tecnologías de la Información, así como el Modelo de Seguridad y privacidad de la Información (MSPI); para dar cumplimiento a la exigencia del Gobierno Nacional de la implementación de la política de Gobierno Digital y la política de Seguridad Digital; propendiendo de igual forma por los derechos como el habeas data, la imagen, la intimidad, el buen nombre y la privacidad.

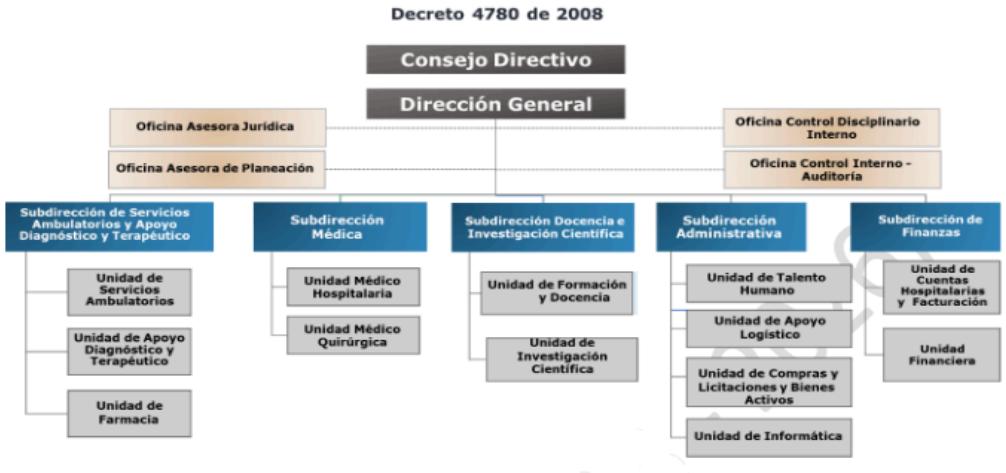
El Plan de Tratamiento de Riesgos se enmarca a nivel de la entidad dentro del objetivo No 3 "Fortalecer la gestión por procesos y cultura de mejoramiento", que busca que el Hospital Militar Central en concordancia con el proceso de fortalecimiento organizacional y el mejoramiento continuo de los procesos desarrolla acciones que facilitan el control y evaluación del cumplimiento a la normatividad, estándares de calidad y alianzas estratégicas con los proveedores en aras de asegurar y optimizar la atención al paciente por medio de los procesos de apoyo como: Tecnologías de la información, gestión logística y gestión de adquisiciones; Específicamente en la estrategia número 3.4 "Optimizar el uso de los sistemas de información para la atención al paciente" que indica "Implementar procesos, metodologías, principios, políticas, estándares y controles que mejoren de forma continua los sistemas de información que faciliten la gestión y administración de la entidad a través de infraestructura tecnológica que garantice la confidencialidad, integridad y disponibilidad de la información para asegurar la prestación idónea en la atención de los pacientes."

6.4 MAPA DE PROCESOS



El HOMIL soporta su operación mediante procesos organizacionales estratégicos, misionales, de apoyo y evaluación, apoyados en estandarización de procedimientos, guías y manuales enfocados en la prestación de servicios con calidad, humanización, seguridad a los usuarios y la comunidad a través de una cultura de mejoramiento continuo; por lo anterior, el Plan de Tratamiento de Riesgos es transversal a todos los procesos y servicios de la entidad.

ORGANIGRAMA



7. CONCEPTOS Y DEFINICIONES

7.1. DEFINICIONES

Riesgo: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

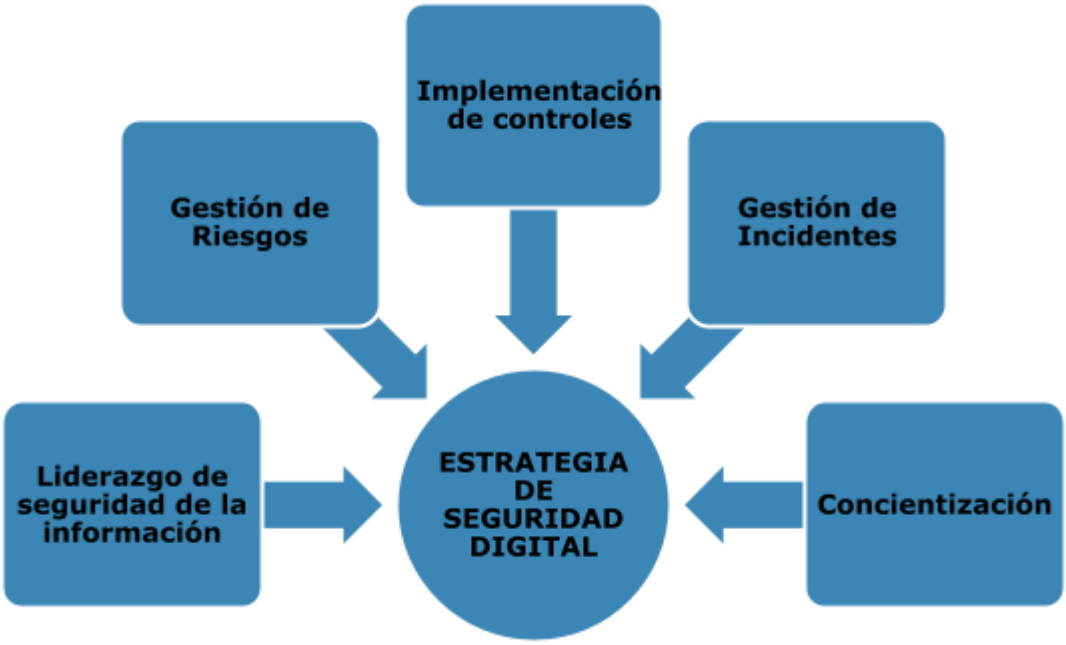
Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Control o Medida: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

8. DESARROLLO

El Hospital Militar Central establecerá una estrategia integral de seguridad digital, que integre los principios, políticas, procedimientos, manuales, formatos y lineamientos necesarios para la gestión de la seguridad de la información. Esta estrategia se desarrollará bajo la premisa de que su implementación se basa en el Modelo de Seguridad y Privacidad de la Información (MSPI), así como en el Plan de Tratamiento de Riesgos de Seguridad de la Información y en el Procedimiento de Gestión de Incidentes, asegurando un marco estructurado y coherente para la identificación, evaluación y tratamiento de los riesgos asociados a los activos de información.

Por tal motivo, El Hospital Militar Central define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Fuente: MINTIC

A continuación, se describe el objetivo de cada una de las estrategias específicas a la Gestión de riesgos de seguridad de la Información:

Proceso de identificación y clasificación de activos de la información

El Hospital Militar Central identificará toda información o todo activo que la contenga así:

- **Información:** Información almacenada, procesada, transmitida física o digitalmente, Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada).

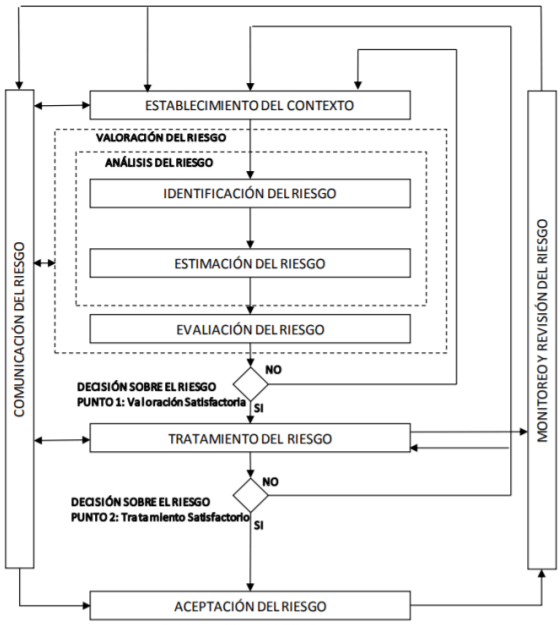
- **Software:** Aplicaciones, herramientas de desarrollo y/o utilidades.
- **Hardware:** son activos físicos como, por ejemplo, equipos de cómputo y de comunicaciones, medios removibles, entre otros que por su criticidad son considerados activos de la información, no solo activos fijos).
- **Servicios:** Servicios de computación y comunicaciones, tales como Internet, correo electrónico, páginas de consulta, directorios compartidos e intranet, entre otros.
- **Personas:** Aquellos colaboradores que, por su conocimiento, habilidades, experiencia y criticidad para el proceso, son consideradas activos de la información.
- **Imagen y reputación:** Good Will o reconocimiento público que debe ser protegido.

Para esta labor todos los responsables de los procesos deberán diligenciar la encuesta publicada de esta manera se definirá la matriz de activos de la información en los siguientes términos:

-Identificación o etiquetado
-Proceso al que corresponde
-Descripción del activo
-Tipo de activo
-Responsable

Una vez identificado y realizado el inventario de activos de la información deberá ser clasificado con base a los criterios de clasificación establecidos dentro de la normatividad vigente y de acuerdo a la política de seguridad de la información definida para la entidad.

Proceso De Valoración De Riesgos De Seguridad De La Información



Fuente: MINTIC

El análisis de riesgos se realizará a todos y cada uno de los procesos estratégicos, misionales, de apoyo y de evaluación del Hospital Militar Central. Los riesgos asociados a la seguridad de la información que se identifiquen a los activos de la información identificados deberán ser tratados conforme los Lineamientos para la Gestión De Riesgos De Seguridad Digital En Entidades Públicas. (2018). Adicionalmente, se dará cumplimiento a la Guía de Administración del Riesgo del Hospital Militar Central.

El análisis y evaluación de riesgos deberá hacerse al ***menos una vez al año*** y cada vez que ocurran cambios significativos en la estructura orgánica de las dependencias y entidades que conforman el Hospital Militar Central, en la plataforma tecnológica, en los procesos, entre otros.

Respecto al seguimiento y consolidación de evidencia se realizará conforme el procedimiento establecido.

Documentación De Resultados

El resultado de esta fase se verá reflejado en una tabla tipo Excel como la que se refleja a continuación y a la cual la Unidad de Informática realizará el seguimiento y monitoreo respectivo.

Identificación del Riesgo																
Referencia	Riesgo	Activo	Descripción del Ries	Amenaza	Causas/Vulnerabilid	Tipo	Consecuencias	Frecuencia	Probabilidad Inherer	%	Impacto Inherente	%	Zona de Riesgo Inhe	Opción de tratamier	N° Control	

Valoración del Riesgo														
Descripción del Control (Actividad de control)	Soporte	Responsable de la Ejecución	Atributos								Impacto Residual (1° Control)	Probabilidad residual (2° Control)	Zona de Riesgo Final	%
			Tipo	%	Implementación	%	Calificación	Documentación	Frecuencia	Evidencia				

Planes de acción (para la opción de tratamiento reducir)					
Plan de Acción	Responsable	Fecha de Implementación	Fecha de Seguimiento	Seguimiento	Estado

9. ROLES Y RESPONSABILIDADES

En alineación con la política de operación para la administración del riesgo de la entidad, se definen las siguientes responsabilidades y los roles de quienes deben ejecutar las actividades así:

ROL	RESPONSABILIDADES
Comité de Gestión y Desempeño Institucional	• Analizar los riesgos, vulnerabilidades, amenazas y escenarios de seguridad de la información que pongan en peligro el cumplimiento de objetivos estratégicos, planes institucionales, metas, compromisos en la entidad y

	la capacidad de prestación de servicio. • Analizar, aprobar y realizar el seguimiento de los resultados del Plan de Tratamiento de riesgos de seguridad de la información para garantizar la misión institucional.
Jefe Oficina Asesora de Planeación	• Consolidar el mapa de riesgos de seguridad de la información. • Acompañar, orientar y capacitar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo.
Jefes de Oficina, Jefes de Unidad, Jefes de Servicio y Supervisores de Contrato	• Adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos de seguridad de la información identificados • Monitorear los riesgos identificados sobre los activos de la información y aplicar los controles definidos en los procesos a su cargo, • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión de riesgo asociado a su responsabilidad y el proceso a su cargo.
Oficina de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Realizar el seguimiento a los riesgos y a la medición del nivel de eficacia de los controles para el tratamiento de riesgos identificados en las áreas en los diferentes niveles de operación de la entidad.
Personal responsable de activos de la información	• Clasificar los activos de información bajo su responsabilidad de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad, verificar que se les proporcione un nivel adecuado de

	protección en conformidad con los estándares, políticas y procedimientos de seguridad de la información. • Definir los acuerdos de niveles de servicio para recuperar sus activos de información y sistemas críticos e identificar los impactos en caso de una interrupción extendida. • Comunicar sus requerimientos de seguridad de información al líder del Área de Seguridad de la Información del Hospital Militar Central. • Determinar y autorizar todos los privilegios de acceso a sus activos de información. • Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información. • Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Estas revisiones podrán realizarse en coordinación con el custodio del activo; sin embargo, se deben verificar los resultados de las revisiones y reportar cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad. • Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.

Oficina de Seguridad Física	• 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. • 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 del Hospital Militar Central.
Área de Gestión de la Seguridad de la Información – Unidad de Informática	• Deberá encargarse de la planeación, control y ejecución del sistema de gestión de seguridad de la información. • Liderar el proceso de identificación y clasificación de activos de la información. • Identificación, analizar, valorar y gestionar los riesgos de seguridad de la información asociados a los activos de la información de la entidad. • Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de la información. • Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información. • Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración.

	• Custodiar la información y los medios de almacenamiento bajo su responsabilidad. • Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.

10. CRONOGRAMA DE TRABAJO

En el Anexo N° 1 del Plan de Seguridad y Privacidad de la Información se presenta el cronograma de actividades y la Gestión de Riesgos de acuerdo al Mapa de Riesgos Institucionales, facilitando la mejora continua del Modelo de Privacidad y Seguridad de la Información (MPSI). En este anexo se detallan las macroactividades, actividades, tareas, responsables, evidencias y fechas de programación. Estas actividades serán objeto de seguimiento trimestral a través del Comité de Gestión y Desempeño Institucional.

11. SEGUIMIENTO

11.1 INDICADORES

El seguimiento al Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia 2026 se realizará en el marco de las reuniones trimestrales del Comité de Gestión y Desempeño Institucional. Adicionalmente, con esta misma periodicidad se efectuará el reporte de monitoreo del Mapa de Riesgos. Dicho seguimiento se realizará a través del siguiente indicador:

Nombre	Descripción
Ejecución de actividades del Plan de Seguridad y Privacidad de la Información	Dentro del Plan de Seguridad y Privacidad de la Información se gestionan los riesgos de seguridad de la información. Se da cumplimiento al

	mapa de riesgos mediante el reporte de Monitoreo del Mapa de Riesgos y el porcentaje de avance de las actividades del plan respecto al avance planteado.

12. COMUNICACIÓN Y CONSULTA

El Plan de Tratamiento de Riesgos de Seguridad de la Información se publicará en la página web de la entidad www.hospitalmilitar.gov.co en la opción Transparencia Institucional, Planeación, Políticas, lineamientos y manuales-Planes estratégicos Institucionales, posterior a la aprobación por el comité de gestión institucional como corresponde a lo indicado por la normatividad. En la intranet institucional se encontrará en planes institucionales disponible para consulta del personal que labora en la entidad.

13. BIBLIOGRAFÍA

- Consejo Nacional de Política Económica y Social (2019). Política Nacional para la Transformación Digital e Inteligencia Artificial. Bogotá, D.C.
- Departamento Nacional de Planeación (2023). Plan Nacional de Desarrollo 2022-2026. COLOMBIA, POTENCIA MUNDIAL DE LA VIDA
- Hospital Militar Central. Política de Seguridad de la Información (2022). Bogotá D.C.
- Ministerio de Defensa Nacional (2023) Plan estratégico Sectorial de tecnologías de la información PETI. Bogotá D.C.
- Ministerio de Tecnologías de la Información y Comunicaciones (2023) Manual de Gobierno Digital. Bogotá, D.C.
- Ministerio de Tecnologías de la información y comunicaciones. Lineamientos del Modelo de Seguridad y Privacidad de la Información (2025). Bogotá D.C.

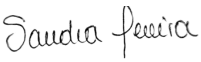
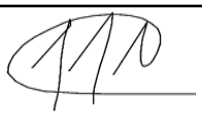
14. ANEXOS

Anexo N° 1. Plan de Seguridad y Privacidad de la información 2026

15. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS DEL CAMBIO	FECHA DEL CAMBIO
ID	ACTIVIDAD			
--	Primera versión del Documento	N.A.	N.A.	01/08/2018
1	Actualización de Actividades	Se actualiza el contenido de actividades a desarrollar en planeación de actividades	Actualización de actividades	01/03/2019
2	Actualización de Formato	Se actualiza el contenido del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualización contenido	Enero 2021
3	Actualización de Actividades	Según los Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas. (2018). https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidad	Resolución 500 de 2021	Diciembre de 2021.

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS DEL CAMBIO	FECHA DEL CAMBIO
ID	ACTIVIDAD			
		es+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b		
4	Actualización de Formato	Se actualiza el contenido del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualización contenido	Enero 2023
5	Actualización de Actividades	Se actualiza el contenido de las actividades del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualización contenido	Enero 2024
6	Actualización de Formato	Se actualiza el contenido del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualización contenido	Noviembre 2024
7	Actualización de Actividades	Se actualiza el contenido de las actividades del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualización contenido	Noviembre 2025
8	Actualización de Formato	Se actualiza el contenido del Plan de Tratamiento de Riesgos de Seguridad de la Información	Actualización contenido	Enero de 2026

APROBACIÓN				
	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
ELABORÓ	Capitán Luis Fernando Sierra Joya	Oficial de Seguridad de la Información	Enero de 2026	
	OPS Sandra Sandra Ximena Pereira Carrero	Ingeniera Especialista GSPI	Enero de 2026	
REVISÓ	Teniente Coronel Eduardo Enrique Mendoza Palacio	Jefe Unidad de Seguridad y Defensa – Unidad de Informática	Enero de 2026	
	Ingeniero José Miguel Cortés García	Seguridad y Defensa – Subdirección Administrativa (E)	Enero de 2026	
APROBÓ	El presente Plan de Tratamiento de Riesgos de Seguridad de la información se encuentra aprobado por el Comité de Gestión y Desempeño de la entidad realizado el 21 de enero de 2026.			
CALIDAD Revisión Metodológica	**SMSM.** Clara Ines Espitia Sanchez	Responsable Área Gestión de Calidad (E)	Enero de 2026