SUBDIRECCIÓN ADMINISTRATIVA
UNIDAD DE INFORMÁTICA
HOSPITAL MILITAR CENTRAL – HOMIL
CÓDIGO: GT-UNIN-PL-04, VERSIÓN: 01
FECHA DE EMISIÓN: 27-01-2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

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

Ingeniera Teresa Moreno Vizcaíno
Jefe de Unidad Seguridad Y Defensa (E)
Subdirección Administrativa
Unidad de Informática
Hospital Militar Central

TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el Hospital Militar Central responde a las necesidades, requisitos de seguridad, procesos, tamaño y estructura propios de la institución. Su objetivo principal es preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando así su correcto uso y la privacidad de los datos.

En línea con este propósito, el Hospital Militar Central (HOMIL) adoptó la Directiva Permanente N° 002 del 15 de junio de 2021, que establece los "Lineamientos para la Implementación de la Política de Gobierno Digital en el Hospital Militar Central". Esta directiva busca alinear el Plan de Seguridad y Privacidad de la Información con las Resoluciones 500 de 2021 y 746 de 2022, emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), así como con el Modelo de Privacidad y Seguridad de la Información de la entidad.

El presente documento detalla el Plan de Seguridad y Privacidad de la Información del Hospital Militar Central, el cual se encuentra alineado con el Plan de Seguridad y Privacidad de la Información del Sector Defensa y con los requerimientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI. Este plan se basa en el Modelo de Seguridad y Privacidad de la Información (MSPI), que a su vez está alineado con el Marco de Referencia de Arquitectura TI y brinda soporte transversal a los demás componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. Además, el Plan de Seguridad y Privacidad de la Información del Hospital Militar Central se adhiere a las buenas prácticas de seguridad establecidas en la norma ISO/IEC 270001:2013, la legislación sobre Protección de Datos Personales, Transparencia y Acceso a la Información Pública, y otras normas pertinentes a la entidad.

La implementación completa de este plan tiene como objetivo proteger toda la información generada, procesada, almacenada y utilizada por el Hospital Militar Central en todos sus procesos, tanto misionales como de apoyo. El propósito fundamental es mantener la confidencialidad, integridad y disponibilidad de los activos de información, asegurando su uso adecuado y la privacidad de los datos. Para lograrlo, el área de Gestión de Seguridad de la Información de la Unidad de Informática continuará trabajando en la mejora continua del MSPI., así:

2. OBJETIVO

2.1 OBJETIVO GENERAL

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Hospital Militar Central, mediante la identificación de oportunidades de mejora en el Modelo de Privacidad y Seguridad, la Política general de seguridad y privacidad de la información y la estrategia de Continuidad de los servicios tecnológicos, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a través de la implementación de estrategias de seguridad digital.

2.2 OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital del Hospital Militar Central.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del MPSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información

3. ALCANCE

El alcance del Plan de seguridad de la información del HOMIL incluye:

- **Fases:** Diagnóstico, Planeación, Operación, Mejora Continua y Evaluación, según el Modelo de privacidad y Seguridad de la Información.
- **Procesos:** Estratégicos, misionales, de apoyo y de evaluación.
- **Tecnologías de la información:** todas las que soportan los servicios tecnológicos que reciben, crean, procesan, gestionan, administran transmiten o resguardan activos de la información.

4. MARCO LEGAL

Al HOMIL para efectos de este Plan de la Seguridad y Protección 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)

Marco Normativo	Descripción
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
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 lineamientos 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

Marco Normativo	Descripción
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.
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 Número 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 Pública 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.

Marco Normativo	Descripción
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.
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

5. ALINEACIÓN ESTRATÉGICA

1. POLÍTICAS, PLANES Y PROGRAMAS INTERNACIONALES, NACIONALES Y SECTORIALES

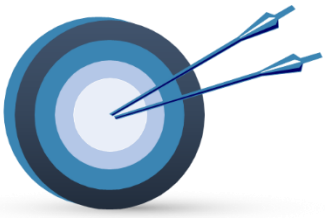
El Plan de Seguridad de la información del Hospital Militar Central está alineado con dos documentos fundamentales:

- La Política de Gobierno Digital, que establece el compromiso del Gobierno Nacional con la transformación digital pública. Esta política busca fortalecer la relación entre el ciudadano y el Estado, mejorar la prestación de servicios por parte de las entidades públicas y generar confianza en las instituciones públicas.
- El Plan Nacional de Desarrollo, específicamente en el artículo 143º, que establece la transformación digital como un motor de oportunidades e igualdad. Este artículo requiere que el Ministerio de Tecnologías de la Información y las Comunicaciones diseñe e implemente una estrategia integral para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en el país. Esta estrategia incluye medidas para fortalecer el Gobierno Digital y promover un entorno digital seguro.

2. MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG

El Plan Estratégico de tecnologías de la información se encuentra alineado al Marco General del Modelo Integrado de Planeación y Gestión con lo relacionado en las políticas de gestión y desempeño institucional Número 12 - Seguridad Digital.

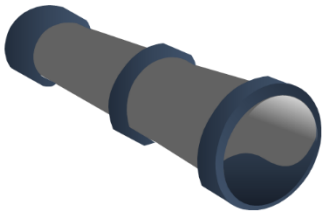
3. PLAN ESTRATÉGICO INSTITUCIONAL



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.

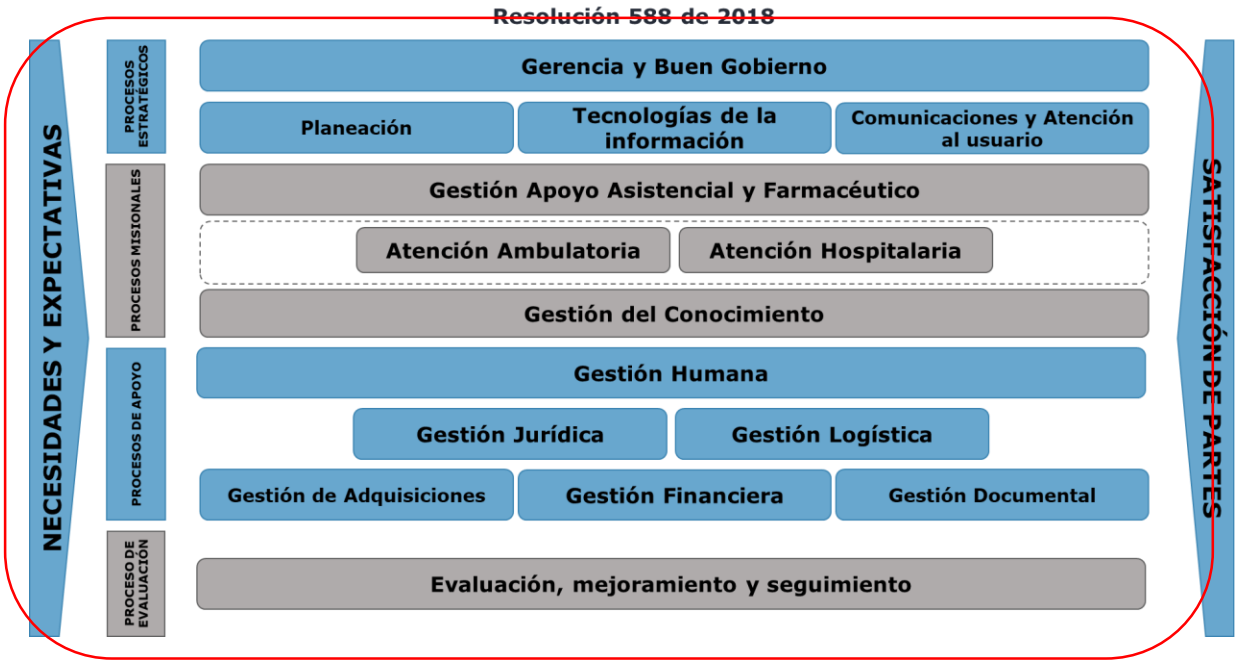
Con el propósito de garantizar la integridad, disponibilidad, confidencialidad y privacidad de la información en sus procesos, la Unidad de Informática en apoyo al Hospital Militar Central ha creado el proceso de transformación e implementación del Plan de Seguridad y Privacidad de la Información, así como el Modelo de Seguridad y Privacidad de la Información (MSPI). Esto se hace para cumplir con el requisito del Gobierno Nacional de implementar el MSPI de la política de Gobierno Digital en la entidad, respetando así los derechos de habeas data, imagen, intimidad, buen nombre y privacidad.

El Plan de Seguridad y Privacidad de la Información se enmarca a nivel de la entidad de la siguiente manera:

- **Dentro de la Mega 2 - Gestión Institucional:**
  - La medición del desempeño institucional es una operación estadística que mide la gestión y el desempeño de las entidades públicas bajo los elementos fundamentales y la estructura temática del Modelo Integrado de Planeación y Gestión (MIPG), así como el avance del Modelo Estándar de Control Interno (MECI). Esto se traduce en la capacidad del HOMIL para orientar sus procesos de Gestión Institucional hacia una mejor prestación de servicios con el fin de resolver efectivamente las necesidades y problemas de los ciudadanos con criterios de calidad, integridad, legalidad y transparencia.
- **Dentro del objetivo No. 3 "Fortalecer la gestión por procesos y cultura de mejoramiento":**
  - 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 de la normatividad, estándares de calidad y alianzas estratégicas con los proveedores con el fin de asegurar y optimizar la atención al paciente a través de procesos de apoyo como las tecnologías de la información, la gestión logística y la gestión de adquisiciones.
  - Específicamente, en la estrategia número 3.4 "Optimizar el uso de los sistemas de información para la atención al paciente", se indica que se deben implementar procesos, metodologías, principios, políticas, estándares y controles que mejoren continuamente los sistemas de información que faciliten la gestión y administración

de la entidad a través de una infraestructura tecnológica que garantice la confidencialidad, integridad y disponibilidad de la información para asegurar una prestación idónea de la atención a los pacientes.

4. MAPA DE PROCESOS



El Hospital Militar Central (HOMIL) sustenta su operación en procesos organizacionales estratégicos, misionales, de apoyo y evaluación, respaldados por la estandarización de procedimientos, guías y manuales centrados en la prestación de servicios de calidad, humanizados y seguros para los usuarios y la comunidad. Estos procesos se sustentan en una cultura de mejora continua. Por lo tanto, el Plan de Seguridad de la Información se extiende a todos los procesos de la entidad.

6. CONCEPTOS Y DEFINICIONES

Información: Información almacenada o procesada 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, 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: Aquellas personas 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.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta el beneficio que se genera.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

7. DESARROLLO

El Hospital Militar Central establecerá una estrategia de seguridad digital para proteger sus activos de información y garantizar la confidencialidad, integridad y disponibilidad de la información. Esta estrategia se basará en los siguientes principios:

- Confidencialidad: La información sólo debe estar disponible para las personas autorizadas.
- Integridad: La información debe ser exacta y completa.
- Disponibilidad: La información debe estar disponible para los usuarios autorizados cuando la necesiten.

La estrategia de seguridad digital del Hospital Militar Central incluirá las siguientes políticas:

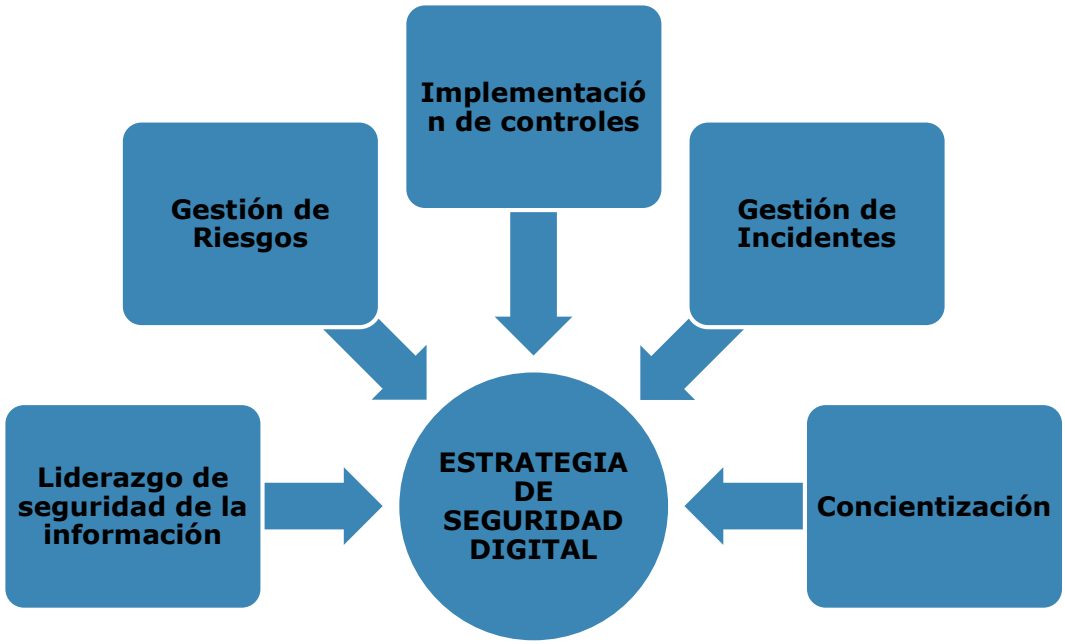
- Política de seguridad de la información: Esta política establecerá los requisitos generales para la protección de la información.
- Política de gestión de riesgos de seguridad de la información: Esta política establecerá el proceso para identificar, evaluar y gestionar los riesgos de seguridad de la información.
- Política de gestión de incidentes de seguridad de la información: Esta política establecerá el proceso para responder a los incidentes de seguridad de la información y mitigar su impacto.

La estrategia de seguridad digital del Hospital Militar Central también incluirá los siguientes procedimientos:

- Procedimiento de gestión de la seguridad de la información: Este procedimiento establecerá los pasos específicos que deben seguirse para proteger la información.
- Procedimiento de gestión de riesgos de seguridad de la información: Este procedimiento establecerá los pasos específicos que deben seguirse para identificar, evaluar y gestionar los riesgos de seguridad de la información.
- Procedimiento de gestión de incidentes de seguridad de la información: Este procedimiento establecerá los pasos específicos que deben seguirse para responder a los incidentes de seguridad de la información y mitigar su impacto.

La estrategia de seguridad digital del Hospital Militar Central también incluirá las siguientes guías:

- Guía de gestión de la seguridad de la información: Esta guía proporcionará orientación sobre cómo implementar y gestionar la estrategia de seguridad de la información.
- Guía de gestión de riesgos de seguridad de la información: Esta guía proporcionará orientación sobre cómo identificar, evaluar y gestionar los riesgos de seguridad de la información.
- Guía de gestión de incidentes de seguridad de la información: Esta guía proporcionará orientación sobre cómo responder a los incidentes de seguridad de la información y mitigar su impacto.



Fuente: MINTIC

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

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.

Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base en un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

PORTAFOLIO DE ACTIVIDADES

Para cada estrategia específica, el Hospital Militar Central define las siguientes actividades, que tienen por objetivo lograr el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**Actividad 1:** Definir roles, responsabilidades y perfiles en la aplicación Dinámica Gerencial y el la suite de colaboración Google WorkSpace. **Actividad 2:** Comunicar y socializar la política general de seguridad de la información. **Actividad 3:** Implementar el "Plan de Sensibilización y Capacitación en Seguridad de la Información"	Actividad 1: Matriz de roles y responsabilidades Actividad 2: Evidencia mensual de socialización. Actividad 3: Evidencias de sensibilización y capacitación en seguridad de la información.
Gestión de riesgos	**Actividad 1:** Identificación de Activos: Utilizar el procedimiento de "Inventario y Clasificación de Activos de Información" (GT-UNIN-	**Actividad 1:** Inventario de activos de la información actualizado a 2025. **Actividad 2:** Documento de análisis de riesgos

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	MN-03) para identificar y clasificar los activos. **Actividad 2:** Análisis de Riesgos: Incluir en el análisis de riesgos las amenazas específicas mencionadas en el manual GT-UNIN-MN-03 (robo de equipos, acceso no autorizado a la red, código malicioso, etc.). **Actividad 3**: Tratamiento de Riesgos: Implementar los controles específicos descritos en el manual GT-UNIN-MN-03 (controles de acceso físico, gestión de usuarios, cifrado de datos, seguridad de la red, etc.).	sobre los activos identificados. **Actividad 3:** Evidencia de Implementación de controles o Plan de implementación.
Concientización	**Capacitación:** Implementar el "Plan de Sensibilización y Capacitación en Seguridad de la Información" (GT-UNIN-MN-03-FT-02) y el programa anual de concientización (GT-UNIN-MN-03). **Concientización:** Difundir la información de seguridad (GT-UNIN-PO-01) a todos los niveles de la entidad.	Evidencias de la Implementación del Plan Evidencias de la Concientización
Implementación de controles	**Control de Acceso:** Aplicar los lineamientos detallados en el manual GT-UNIN-MN-03 (control de acceso físico a áreas	**Control de Acceso:** Evidencia de la aplicación del Control.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	protegidas, gestión de usuarios y contraseñas, restricción de acceso a la información, etc.). **Gestión de Usuarios**: Seguir el procedimiento "Gestión de Usuarios y Contraseñas" (GT-UNIN-MN-03) para la creación, modificación y eliminación de cuentas. **Protección de Datos:** Implementar mecanismos de cifrado (GT-UNIN-MN-03) para la información sensible, cumpliendo con la Ley 1581 de 2012 (GT-UNIN-MN-03). **Seguridad de la Red:** Segmentar la red (GT-UNIN-MN-03) y configurar firewalls, sistemas de detección de intrusos y antivirus. **Desarrollo Seguro:** Cumplir con los lineamientos de desarrollo seguro (GT-UNIN-MN-03) y realizar pruebas de seguridad en las aplicaciones.	**Gestión de Usuarios**: Evidencia de la aplicación del Control. **Protección de Datos:** Evidencia de la aplicación del Control. **Seguridad de la Red:** Evidencia de la aplicación del Control. **Desarrollo Seguro:** Evidencia de la aplicación del Control.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de incidentes	**Definición de Incidentes**: Utilizar el procedimiento de "Gestión de Incidentes de Seguridad" (GT-UNIN-MN-03) para la identificación, reporte y clasificación de incidentes. **Respuesta a Incidentes:** Escalar los incidentes al CSIRT del Sector Defensa (GT-UNIN-PO-01) cuando sea necesario. **Análisis Post-Incidente:** Registrar los incidentes (GT-UNIN-PO-01) y preservar la evidencia (GT-UNIN-MN-03) para investigar las causas y tomar medidas preventivas.	Evidencia de la aplicación del Procedimiento.
Monitoreo y Mejora Continua	**Auditorías:** Realizar auditorías internas (GT-UNIN-MN-03) y externas para evaluar el MPSI (GT-UNIN-PO-01).	Informes de Auditorías y escaneos de Vulnerabilidades

8. ROLES Y RESPONSABILIDADES

El HOSPITAL MILITAR CENTRAL, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.):

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Comité de Gestión y Desempeño	• Aprobar y hacer seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI. • Aprobar los recursos necesarios para la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información. • Conocer los resultados de los estudios, análisis y recomendaciones en materia de seguridad y privacidad de la información y generar las recomendaciones necesarias.
Unidad de Informática	• Liderar las acciones necesarias para establecer, implementar, mantener y mejorar la Seguridad de la Información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información - MSPI, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas. • Conformar y liderar el equipo de respuesta a emergencias informáticas y centros de operaciones de seguridad con el fin de apoyar la gestión de incidentes de seguridad informática que se llegasen a presentar en el Hospital Militar Central. • Implementar y gestionar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Establecer, verificar, monitorear y validar los procedimientos de continuidad y de contingencia para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	• Establecer, documentar y dar mantenimiento a los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías de información administrada por esta unidad.
Oficial de Seguridad Digital	• Analizar, definir, documentar y gestionar el plan de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidos y aprobados por el Hospital Militar Central. • Elaborar los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información en el Hospital Militar Central y presentarlos para aprobación. • Elaborar el Plan de Sensibilización y Comunicación en Seguridad de la Información.
Talento Humano	• Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta y contratistas dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información. • Gestionar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente. • Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Unidad de Compras, Licitaciones y bienes Activos	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Oficina de Control Interno	• Incluir el tema de seguridad de la información, como un tema a evaluar en cada una de las auditorías a realizar. • Intervenir en situaciones de posibles violaciones a las políticas de seguridad de la información.
Comunicaciones y Relaciones Públicas	• Incluir las actividades de comunicación y sensibilización relacionadas dentro del Plan de Sensibilización y comunicación de Seguridad de la información dentro del Plan Anual de Comunicaciones. • Realizar las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.
Oficina Asesora Jurídica	• Brindar asesoría a los procesos del Hospital Militar Central en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	• Asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
Área 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.
Responsables de los activos de información (Jefes de Área y/o Unidad, Jefes de Oficina, Subdirectores)	• Dar cumplimiento a las políticas y procedimientos de seguridad de la información que se definan como parte del MSPI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros). • 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. • Definir los requerimientos de continuidad y de recuperación en caso de desastre.
Todos los funcionarios y contratistas	• Interactuar junto a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. • Reportar de manera inmediata y a través de los canales establecidos la sospecha u ocurrencia de eventos considerados incidentes de seguridad de la información,

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad de la Información.

9. CRONOGRAMA

Anexo N° 1 - Plan de Seguridad de la información_2025

10. SEGUIMIENTO

El seguimiento al Plan de Seguridad de la información – PSI para la vigencia 2025 se realizará desde la reunión trimestral del comité de gestión y desempeño institucional a través de la medición de los siguientes indicadores:

Nombre	Descripción
Ejecución de actividades del Plan de seguridad y Privacidad de la información	Mide el porcentaje de avance de las actividades del plan respecto al avance planteado.
Cubrimiento del MPSI -Activos de la Información	Mide el cubrimiento de los activos identificados como críticos dentro de la entidad.
Apropiación de Plan de seguridad y privacidad de la información	Mide la apropiación de los funcionarios de la entidad en cuanto al conocimiento y desarrollo de las actividades del plan de seguridad y privacidad de la información.

11. COMUNICACIÓN Y CONSULTA

El Plan de Privacidad y 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.

12. BIBLIOGRAFÍA

El Plan de Privacidad y Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

1. Decreto 612 (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". Presidencia de la República.
2. Resolución 500 (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. Ministerio de Tecnologías de la Información y Comunicación.
3. Manual de Gobierno Digital (2023). Documento que establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y servicios ciudadanos digitales). Ministerio de Tecnologías de la Información y Comunicación.
4. Modelo de Seguridad y Privacidad de la Información (2023). Lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. Ministerio de Tecnologías de la Información y Comunicación.

13. ANEXOS

Anexo N° 1. Cronograma Plan de Seguridad y Privacidad de la información 2025
Anexo N° 2. Directiva permanente N° 002 del 15 de junio de 2021

14. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVO DEL CAMBIO	FECHA DEL CAMBIO
ID	ACTIVIDAD			
1	Primera versión del Documento	N.A.	N.A.	Marzo de 2022
2	Actualización general del documento	Se realiza actualización por parte de la Unidad de Informática teniendo en cuenta lineamientos del Plan de Seguridad y Privacidad de la Información	Mejoramiento continuo	Noviembre de 2022
3	Actualización general del Documento	Aplicación del modelo de Privacidad y Seguridad de la información. Inclusión de la resolución 7870 de Diciembre de 2022	Mejoramiento continuo Imperativo Legal	Enero de 2023
4	Actualización general del Documento	Aplicación del modelo de Privacidad y Seguridad de la información Inclusión de auditorías internas a proveedores HOMIL	Mejoramiento continuo Imperativo Legal	Enero de 2024
5	Actualización general del Documento	Aplicación del modelo de Privacidad y Seguridad de la información. Inclusión de auditorías internas a proveedores HOMIL	Mejoramiento continuo Imperativo Legal	Diciembre de 2024

APROBACIÓN				
	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
ELABORÓ	Ingeniera Teresa Moreno Vizcaíno	Jefe Unidad de Seguridad y Defensa (E) – Unidad de Informática	Enero de 2025	
REVISÓ	Ingeniero José Miguel Cortés García	Seguridad y Defensa – Subdirección Administrativa (E)	Enero de 2025	
APROBÓ	El presente Plan se encuentra aprobado por el Comité Institucional de Gestión y Desempeño **(Acta de Aprobación del 27 de enero 2025)**			
CALIDAD Revisión Metodológica	**MY.** Sildrey Yeigleiza Arenas Vesga	Oficial de Comisión Administrativa permanente en la administración pública – Responsable Área de Gestión de Calidad	Enero de 2025