Ing. Fabio Alberto Alvarado Rodríguez
Jefe de Unidad de Seguridad y Defensa
Unidad de Informática - GESU
HOSPITAL MILITAR CENTRAL – HOMIL
Fecha de Emisión: 25-01-2023

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en el Hospital Militar central está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Por lo anterior el Hospital Militar Central – HOMIL, adoptó 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”; a fin de que el Plan de Seguridad y Privacidad de la Información estuviera alineado a las resoluciones 500 de 2021 y 746 de 2022 expedidas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC y al Modelo de Privacidad y Seguridad de la Información de la entidad.

El presente documento contiene el Plan de Seguridad y Privacidad de la Información del Hospital Militar Central; el cual está alineado al Plan de seguridad y privacidad de la información del Sector Defensa y a lo solicitado por el 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, según lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. Así mismo, el Plan de Seguridad y Privacidad de la información del Hospital Militar Central está acorde con las buenas prácticas de seguridad conforme a la norma ISO/IEC 270001:2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, y demás normas que aplican a la entidad.

La implementación total de este plan busca en todo momento salvaguardar toda la información creada, procesada, custodiada y utilizada por el Hospital Militar Central en todos los procesos Misionales y de apoyo. Siempre con el ánimo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. Por tal Razón a través del área de Gestión de la seguridad de la Información de la Unidad de Informática se seguirá con el mejoramiento del MPSI, así:

Diagnóstico: Se realiza un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI

Planificación: Se determinan las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Operación: Donde se implementan los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.

Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

OBJETIVO

Identificar las oportunidades de mejora al Modelo de Privacidad y Seguridad del Hospital Militar Central, la Política general de seguridad y privacidad de la información y la estrategia de Continuidad de los servicios tecnológicos; con el fin de priorizar aquellas actividades que impacten de manera directa la consecución de los objetivos se seguridad digital del HOMIL.

ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información del HOMIL, Aborda las fases de Diagnostico, Planeación, Operación, Mejora Continua y Evaluación de acuerdo a lo establecido en el Modelo de privacidad y Seguridad de la Información; el cual contempla todos los procesos estratégicos, misionales, de apoyo y de evaluación; y a las tecnologías de la información que soportan los servicios tecnológicos que reciben, crean, procesan, gestionan, administran transmiten o resguardan activos de la información.

MARCO LEGAL

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

Tipo	Número	Fecha de expedición	Origen	Organismo Emisor	Descripción
Ley	80	1993	Nacional	Presidencia	Estatuto general de contratación de la administración pública
Ley	87	1993	Nacional	Presidencia	Control Interno en los organismos del Estado
Ley	527	1999	Nacional	Congreso de la República	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley	1747	2000	Nacional	Presidencia	Reglamenta parcialmente la ley 527 de 1999
Ley	594	2000	Nacional	Congreso de la República	Ley General de Archivos
Ley	599	2000	Nacional	Congreso de la República	Código Penal Colombiano
Ley	603	2000	Nacional	Congreso de la República	Control de legalidad del software
Ley	734	2002	Nacional	Congreso de la República	Código Disciplinario Único

Ley	836	2003	Nacional	Congreso de la República	Régimen Disciplinario FF.MM
Ley	1015	2006	Nacional	Congreso de la República	Régimen Disciplinario para la Policía Nacional
Ley	1266	2008	Nacional	Congreso de la República	Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información
Ley	1273	2009	Nacional	Congreso de la República	Protección de la Información y de los Datos
Ley	1581	2012	Nacional	Congreso de la República	Por la cual se dictan disposiciones generales para la protección de datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013
Decreto	1377	2013	Nacional	Presidencia	por el cual se reglamenta parcialmente la Ley 1581 de 2012
Ley	1712	2014	Nacional	Congreso de la República	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	103	2015	Nacional	Congreso de la República	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto	1083	2015	Nacional	Presidencia	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital
Decreto	1078	2015	Nacional	Presidencia	Decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones
Ley	1915	2018	Nacional	Congreso de la República	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos. Articulo 13 numeral d y numeral i
Decreto	612	2018	Nacional	Presidencia	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

Directiva	10	2019	Nacional	Procuraduría General de la Nación	PGN Protección de Datos
Resolución	500	2021	Nacional	Min TIC	Resolución Mintic – Modelo de Seguridad y Privacidad de la Información
Decreto	88	2022	Nacional	Min TIC	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
Resolución	746	2022	Nacional	Min TIC	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
Resolución	7870	2022	Sectorial	Min Defensa	Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades descritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.

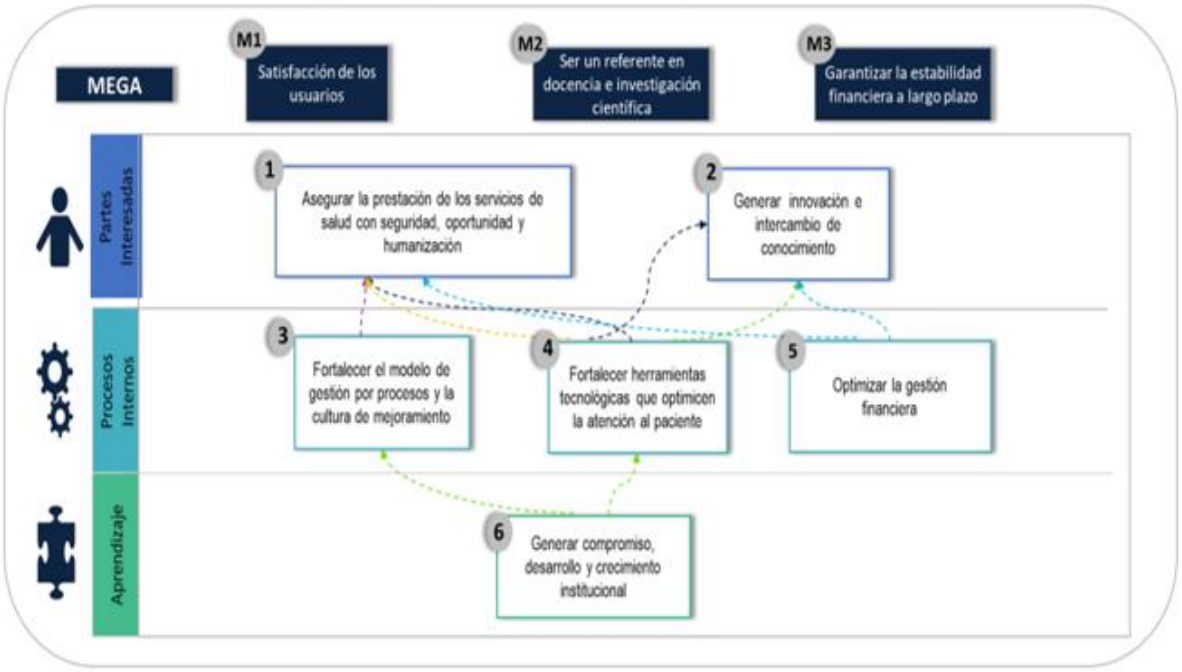
JUSTIFICACIÓN

Con el ánimo de asegurar la integridad, disponibilidad, confidencialidad y privacidad de la información de sus procesos, la Unidad de Informática en apoyo a los procesos del Hospital Militar Central genera 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); para dar cumplimiento a la exigencia del Gobierno Nacional de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital así como la implementación del mismo en la entidad, propendiendo de igual forma por los derechos como el habeas data, la imagen, la intimidad, el buen nombre y la privacidad.

METODOLOGÍA

Objetivos Estratégicos De La Entidad

Mapa Estratégico del Hospital Militar Central 2019-2022



El Plan de Seguridad y Privacidad de la Información se enmarca a nivel de la entidad dentro del objetivo No 4 “Fortalecer Herramientas que optimicen la atención al paciente”, que busca el fortalecimiento de la cobertura en la infraestructura tecnológica, por tanto, el manejo de la seguridad de la información que se maneja a través de esos elementos.

Componentes

Política General De Seguridad De La Información

El HOSPITAL MILITAR CENTRAL, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Modelo de Privacidad y Seguridad de la Información (MPSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

El HOSPITAL MILITAR CENTRAL en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

Objetivo General

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.

Objetivos De La Política General De Seguridad De La Información

- Objetivo 1. Establecer los lineamientos, procedimientos e instructivos en materia de seguridad de la información; adoptado las guías emitidas por el MINTIC en materia de seguridad digital.
- Objetivo 2. Minimizar el riesgo de seguridad digital de todos los procesos de la entidad, por medio de la aplicación de la metodología de análisis de riesgo definida por la entidad.
- Objetivo 3. Mejorar continuamente el modelo de seguridad y privacidad de la información - MSPI, realizando una valoración de forma anual del estado de madurez de la Seguridad de la Información; aplicando el instrumento de evaluación del MPSI publicado por el Min TIC.
- Objetivo 4. Implementar los controles tecnológicos necesarios para la protección de los activos de la información de la entidad y para la reducción de los riesgos de seguridad digital.
- Objetivo 5. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del HOSPITAL MILITAR CENTRAL, mediante la ejecución del Plan de Sensibilización en Seguridad de la Información de la entidad.

NOTA: Las actividades relacionadas con el cumplimiento de los objetivos se encuentran enmarcadas el Plan de Seguridad y Privacidad de la Información de la entidad.

Compromiso De La Alta Dirección General

La Alta Dirección General del HOSPITAL MILITAR CENTRAL se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información (MSPI); así mismo, se compromete a revisar el avance de la implementación del SGSI de

manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

Aplicabilidad

El Modelo de Privacidad y Seguridad de la Información del HOMIL, aplica a todos los niveles funcionales y organizacionales del Hospital Militar Central, a todos sus funcionarios, contratistas, proveedores, operadores, estudiantes, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Hospital Militar Central compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a la entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, el Modelo de Privacidad y Seguridad de la Información aplica a toda la información creada, procesada o utilizada por el Hospital Militar Central, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

GENERALIDADES

Términos 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 auditoria 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 en 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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

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 eestablecer, 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.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	• 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. • 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 definidas 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 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.

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

IMPLEMENTACIÓN

PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

En el Anexo N° 1 se definieron las siguientes actividades con las cuales se establece el plan de seguridad y privacidad de la información, permitiendo así la mejora continúa del Modelo de Privacidad y Seguridad de Seguridad de la Información – MPSI. En el Anexo N° se encuentran relacionadas las Macro Actividades, Actividades, tareas, responsables, evidencias y Fechas de programación. Actividades que se les realizará seguimiento de manera trimestral a través del Comité de Gestión y Desempeño Institucional.

SEGUIMIENTO

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.

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.

BIBLIOGRAFÍA

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

- 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”, donde se encuentra el presente Plan de Privacidad y Seguridad de la Información como uno de los requisitos a desarrollar para cumplir con esta normativa.
- 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”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

ANEXOS

Cuadro Excel - Anexo N° 1 – Plan de Seguridad Y Privacidad de la información

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS 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

APROBACIÓN				
	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	Ingeniero Fabio Alberto Alvarado Rodriguez	Jefe Unidad de Seguridad Y Defensa – Unidad de Informática	Enero de 2023	
REVISÓ	TC (RA) Ricardo Arturo Hoyos Lanziano	Subdirector de Seguridad y Defensa – Subdirección Administrativa	Enero de 2023	
APROBÓ	El presente Plan de Seguridad y privacidad de la información se encuentra aprobado por el Comité de Gestion y Desempeño de la entidad realizada el Dia 19 de enero de 2023			
PLANEACIÓN – CALIDAD Revisión Metodológica	SMSM. Pilar Adriana Duarte Torres	Servidor Misional de Sanidad Militar - Área Gestión de Calidad	Enero de 2023	