PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

UNIDAD DE INFORMATICA - Fecha actualización: 17/01/2022

HOSPITAL MILITAR CENTRAL – HOMIL

TABLA DE CONTENIDO

1. INTRODUCCIÓN

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 la resolución 500 de 2021 y 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, transmitida, 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.

2. OBJETIVOS

Definir las actividades del plan de Seguridad y Privacidad de la Información para la implementación, gestión, verificación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI del Hospital Militar Central.

3. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a todos los procesos del Hospital Militar Central, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI.

4. MARCO LEGAL

Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Alcance
Ley	527	17 Agosto 1999	Externo	MINTIC	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	594	14 Julio de 2000	Externo	Archivo General de La Nación	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Decreto	1747	2000	Externo	MINTIC	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: “Las entidades de certificación, los certificados y las firmas digitales”.
Ley	962	6 septiembre 2005	Externo	DAFP	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley	1273	2009	Externo	MINTIC	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

Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Alcance
					disposiciones
Ley	1341	2009	Externo	MINTIC	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.
Decreto	4890	2011	Interno	Mindefensa	Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional y Se dictan otras disposiciones.
Decreto	19	2012	Externo	DAFP	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
Decreto	2609	2012	Externo	Archivo General de la Nación-MINTIC	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Resolución	1374	2012	Interno	MinDefensa	Por la cual se adiciona la resolución 127 de 2012 “Por la cual se crean y organizan Grupos Internos de Trabajo del Ministerio de Defensa Nacional”.
Decreto	1377	2013	Externo	MINTIC	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales
Decreto	2573	2014	Externo	MINTIC	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.
Ley	1712	2014	Externo	MINTIC	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.
Resolución	10584	2014	Interno	Mindefensa	Por la cual se modifica parcialmente la resolución 1374 de 2012, - para ajustar las funciones del Grupo de Tecnología de Información y las Comunicaciones TIC.

Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Alcance
Ley	1753	2015	Externo	Presidencia de la Republica - DAP	Por la cual se expide el Plan Nacional de Desarrollo 2014 - 2018.
Decreto	103	2015	Externo	Presidencia de la Republica	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto	1078	2015	Externo	MINTIC	Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones – Título 9 – Capítulo I.
Decreto	415	2016	Externo	Función Publica	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	4780	2008	Interno	Mindefensa.-GSED	Por el cual se modifica la estructura del Hospital Militar Central y se dictan otras disposiciones
Resolución	84	2018	Interno	Homil	Por la cual se actualiza la estructura de grupos internos de trabajo
Resolución	588	2018	Interna	Homil	Por la cual se adopta el modelo de operación por procesos “Mapa de Procesos” en el Hospital Militar Central y se dictan otras disposiciones.
Resolución	500	2021	Externa	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.

5. JUSTIFICACIÓN

Con el ánimo de asegurar la integridad, disponibilidad, confidencialidad y privacidad de la información de sus procesos estratégicos, misionales, de apoyo y de evaluación; la Unidad de Informática genera el proceso de transformación e implementación del Plan de Seguridad y Privacidad de la información (MSPI), así como el Sistema de Seguridad de la Información (SGSI), 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 Sistema de Gestión de Seguridad de la Información, propendiendo de igual forma por los derechos como el habeas data, la imagen, la intimidad, el buen nombre y la privacidad.

6. ALINEACIÓN ESTRATÉGICA

6.1. OBJETIVOS ESTRATEGICOS DE LA ENTIDAD

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

6.2. Política de seguridad de la información del hospital militar central

El Hospital Militar Central Diseñará, implementará y mantendrá un sistema de gestión de seguridad de la Información que garantice el cumplimiento de la normatividad vigente, garantice la correcta y adecuada gestión de riesgos de seguridad de la información, que garantice la disponibilidad a los autorizados, la confidencialidad y la integridad de toda la información física o digital clínica de nuestros usuarios, que cumpla con los objetivos de la organización y del sistema de gestión de seguridad de la información y sobre todo se preocupe por mantener adecuada gestión y mejora continua.

6.2.1. Objetivos del SGSI

1. Fortalecer la cultura de seguridad de la información en todas las partes interesadas con el ánimo de garantizar la continuidad del negocio frente a riesgos relacionados con seguridad de la información.

2. Minimizar el riesgo en las funciones más importantes de la entidad, cumpliendo con los principios de seguridad de la información y los principios de la función administrativa.

3. Mantener la confianza de sus usuarios, directivos y empleados, apoyando la innovación tecnológica y protegiendo los activos de TI y los activos de la información.

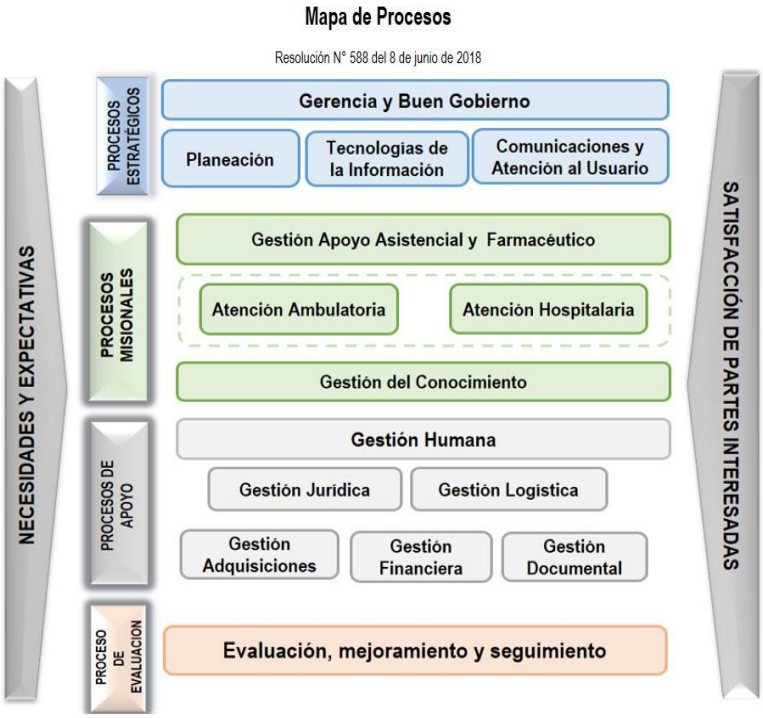
4. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

5. Cumplir las normatividades legales y reglamentarias vigentes y a la cual el Hospital Militar Central debe estar alineado.

6. Planear y fomentar la mejora continua en el sistema de gestión de seguridad de la información.

6.2.2. Alcance del SGSI

El Sistema de Gestión de Seguridad de la Información del Hospital Militar Central será aplicable a todos los procesos estratégicos, misionales, de apoyo y de evaluación propios o de terceros que creen, procesen, transmitan o resguarden información clínica de nuestros usuarios; esto con el ánimo de garantizar la disponibilidad, confidencialidad e integridad de esta información.



7. GENERALIDADES

7.1. TERMINOS 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).

8. ROLES Y RESPONSABILIDADES

8.1. LIDERAZGO

La dirección General del Hospital Militar Central a través del comité institucional de gestión y desempeño liderará las funciones relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, por medio de un acto administrativo. Con el propósito de garantizar el éxito de su implementación, y dar cumplimento entre otras, a las siguientes acciones:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la Entidad.
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI.

8.2. Responsable del MSPI

8.2.1 Líder del Área de Seguridad de la Información: para este rol será designado un funcionario del Hospital Militar Central y será el responsable por la definición, implementación, operación, mantenimiento y mejoramiento del Sistema de Gestión de Seguridad de la Información.

Perfil: Ingeniero de sistemas, electrónico o afines, mínimo con especialización en seguridad informática o de la información. Sus principales funciones serán:

- Ejecutar las tareas de seguridad de la información que le asigne el Comité de Seguridad de la Información.
- Mantener informado al Comité de Seguridad de la Información, sobre los eventos e incidentes de seguridad que se presenten al interior de la misma.
- Gestionar la actualización del Sistema de Gestión de Seguridad de la Información.
- Definir la estrategia de gestión de los riesgos de seguridad de la información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.
- Definir, documentar, mantener, divulgar y actualizar los procedimientos propios de la gestión del Sistema de Gestión de Seguridad de la Información.
- Supervisar el cumplimiento de los procedimientos del Sistema de Gestión de Seguridad de la Información.
- Promover la creación y actualización de las políticas y estándares de seguridad de la información y velar por el cumplimiento de las mismas.
- Apoyar la consolidación de la cultura de seguridad de la información entre todo el personal.
- Coordinar la difusión de cualquier comunicación relacionada con el Comité de Seguridad de la Información.

- Participar activamente en las actividades convocadas por el Comité de Seguridad de la Información.
- Coordinar la realización periódica de auditorías internas y pruebas de vulnerabilidad de acuerdo con las políticas establecidas, previa autorización del Comité de Seguridad de la Información.
- Elaborar y proponer al Comité de Seguridad de la Información, planes, procedimientos y controles para el mejoramiento del Sistema de Gestión de Seguridad de la Información.
- Proponer al Comité de Seguridad de la Información, planes de capacitación, concientización y entrenamiento para difundir las políticas, normas y estándares de seguridad de la información al personal.
- Apoyar y coordinar el desarrollo de actividades de investigación y búsqueda de información referente a seguridad de la información.
- Elaborar los informes que le sean requeridos por el Comité de Seguridad de la Información sobre el Sistema de Gestión de Seguridad de la Información de la dependencia o entidad.
- Coordinar la implementación de acciones preventivas y correctivas del Sistema de Gestión de Seguridad de la Información con los respectivos responsables, de acuerdo con los resultados de las auditorías internas o externas.
- Implementar y hacer seguimiento al plan de mejora continua del Sistema de Gestión de Seguridad de la Información.
- Liderar el proceso de certificación y recertificación.
- Proponer y apoyar proyectos de seguridad de la información.

8.2.2 Oficial o promotor de Seguridad de la Información: para este rol será designado un funcionario del Hospital Militar Central y será el apoyo para el Jefe de la Unidad de Informática en la implementación de las actividades y controles necesarios para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de la Información.

Perfil: Técnico, tecnólogo ó ingeniero, en el área de sistemas, electrónica o afines, con capacitación básica en seguridad de la información y/o en la norma ISO 27000. Sus principales funciones serán:

- Desarrollar campañas de sensibilización y concientización que garanticen el fortalecimiento de la cultura de seguridad de la información entre todos los funcionarios.
- Velar por la difusión y cumplimiento de las políticas y estándares de Sistema de Gestión de Seguridad de la Información.
- Asesorar y recomendar al líder de Seguridad de la Información y dueños de procesos en temas relacionados con la Seguridad de la Información.
- Apoyar al jefe de la Unidad de informática, en la implementación técnica y operativa de controles de seguridad de la información pertinentes al proceso del Sistema de Gestión de Seguridad de la Información.
- Apoyar a las áreas de tecnología en el proceso de análisis y evaluación de riesgos.
- Realizar la gestión de incidentes de seguridad y reportarlos al líder de Seguridad de la Información.
- Apoyar al Líder del Área de Seguridad de la Información durante la ejecución de las auditorías internas o externas al Sistema de Gestión de Seguridad de la Información.
- Será el responsable de evaluar y autorizar las solicitudes de conexiones remotas y demás acceso externo a la plataforma tecnológica del Hospital Militar Central.

El Comité de Seguridad de la información deberá realizar sesiones periódicas mínimo una vez al año y cada vez que se requieran, la participación en estas sesiones es obligatoria para el Jefe de la Unidad de Informática, el líder del área de seguridad de la información, el oficial de seguridad, para el representante de la oficina de control interno y, en los casos en que aplique el representante de la oficina jurídica y el representante de la oficina de seguridad.

Sus principales funciones serán:

- Estructurar, evaluar y presentar estrategias y proyectos ante la alta dirección que permitan fortalecer la seguridad de la información del Hospital Militar Central.
- Revisar en el marco de las sesiones ordinarias con frecuencia anual, o extraordinarias cuando las circunstancias así lo requieran, los aspectos relativos a las estrategias, protocolos y procedimientos aplicados o propuestos por sus integrantes en materia de seguridad de la información.
- Gestionar las actividades de promoción y difusión de la cultura de seguridad de la información contenida en el presente documento.
- Supervisar la gestión desarrollada por el líder del Grupo de Seguridad de la Información en la dirección del Sistema de Gestión de la Seguridad de la Información del Hospital Militar Central.
- Gestionar la adquisición de soluciones o herramientas que apoyen la seguridad de la información y realizar el trámite ante el Comité de Integración de Tecnologías de la Información - CITI.
- Estudiar y conceptuar sobre los casos especiales de seguridad de la información que se presenten y afecten al Hospital Militar Central, para recomendar las acciones pertinentes y apoyar la toma de decisiones.
- Avalar los planes de pruebas y análisis de vulnerabilidades externas e internas a los componentes de la plataforma tecnológica, con el fin de garantizar un alto nivel de seguridad y que se cuente con las herramientas adecuadas para la protección de la misma.
- Definir el estándar para realizar el levantamiento del inventario de activos de información, la clasificación y la rotulación de los mismos, de acuerdo con su nivel de confidencialidad y criticidad.
- Establecer la metodología para el análisis de riesgos, donde se identifiquen los activos de información críticos, su impacto, las amenazas, vulnerabilidades y probabilidad de ocurrencia, y se establezcan las respuestas necesarias para su tratamiento.
- Mantener actualizada las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información de acuerdo a la estrategia sectorial del Ministerio de Defensa Nacional.
- Reportar al Comité de Seguridad de la Información Sectorial aquellos casos que requieran la intervención de este.

8.3. ROLES, RESPONSABILIDADES Y AUTORIDADES

8.3.1. Director General

1. Verificar el cumplimiento del presente documento, en particular la difusión y adopción de las políticas, normas y estándares de seguridad de la información.
2. Promover el desarrollo de una cultura de seguridad de la información a través de campañas de sensibilización y concientización.
3. Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información.
4. Apoyar los programas de capacitación, actualización y entrenamiento técnico del personal de la Unidad de Informática en temas relacionados con seguridad de la información.
5. Nombrar al oficial de seguridad de la información (OSI) como integrante del Comité de Seguridad de la Información y apoyar las iniciativas de seguridad que se definan sobre los activos de información.
6. Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del sistema de gestión de seguridad de la información.
7. Ordenar la inclusión de temas relacionados con seguridad de la información en las materias de tecnología que se dictan en las escuelas de formación y capacitación.
8. Apoyar la aplicación y cumplimiento de las recomendaciones emitidas por el comité de seguridad de la información.

8.3.2. Área de Gestión de la Seguridad de la Información – Unidad de Informática

1. Deberá encargarse de la planeación, control y ejecución del sistema de gestión de seguridad de la información.
2. Mantener informado al comité de seguridad de la información y a la dirección general acerca del desempeño del sistema de gestión de seguridad de la información.
3. Liderar el proceso de identificación y clasificación de activos de la información.
4. Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de la información.
5. Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.
6. Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.
7. Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de seguridad de la información desde el diseño.
8. Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
9. Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración.
10. Definir e implementar la estrategia de concientización y capacitación en seguridad de la información para los funcionarios, contratistas y demás terceros, cuando aplique.
11. Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
12. Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.
13. Gestionar la plataforma tecnológica que soporta los procesos de la entidad.
14. Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizan el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
15. Gestionar la adquisición de software y hardware.

16. Asignar los equipos de cómputo a los funcionarios y/o contratistas.
17. A través del áreas de Seguridad de la Información se debe:

- Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
- 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 oficina.
- Gestionar los incidentes de seguridad de la información que se presenten en la organización.
- Realizar análisis de vulnerabilidades a la plataforma tecnológica con el fin de generar recomendaciones.
- 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.

8.3.3. Oficina de Control Interno

1. Deberá velar por el cumplimiento de la política de Seguridad.
2. Deberá hacer cumplir las multas y sanciones equivalentes por incumplimiento de la Política.
3. Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en este documento, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.
4. Realizar auditorías a los procesos del Sistema de Gestión de Seguridad de la Información por lo menos una vez al año, de acuerdo con lo establecido en la norma ISO 27001.

8.3.4. Área de Comunicaciones

1. Deberá divulgar la política de seguridad de la información generando las campañas correspondientes.

8.3.5. Responsables de los activos de la información

1. Identificar, clasificar y custodiar los activos de la información.

8.3.6. Unidad De Talento Humano

1. Comunicar los derechos y establecer las responsabilidades legales que adquiere cada funcionario, contratista y/o tercero, con relación al manejo y protección de los datos institucionales tanto al interior como fuera de las instalaciones del Hospital Militar Central (políticas de seguridad de la información).
2. Incluir en los contratos cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad en el cumplimiento de la política de seguridad de la información del Hospital Militar Central.
3. Garantizar que se realicen las verificaciones y controles de seguridad requeridos por la criticidad del empleo, tales como verificación de antecedentes judiciales, validación de certificados de estudios presentados, validación de referencias de comportamiento satisfactorio y validación de su hoja de vida.

4. Definir claramente las funciones y tareas que desempeñará el funcionario en el cargo con el fin de establecer la responsabilidad en el manejo de la información teniendo en cuenta la clasificación de la misma y el cumplimiento de las políticas de seguridad de la información.
5. Elaborar y ejecutar programas de inducción y de reinducción para los funcionarios asegurando que conozcan sus responsabilidades e implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público.
6. Gestionar los aspectos de seguridad que se requieran durante el proceso de desvinculación de cualquier empleado, y demás novedades de personal, informando a la Unidad de Informática con el fin de que se tomen las medidas y procedimientos de entrega de hardware, software e información a su cargo, necesarios para evitar riesgos que atenten contra la seguridad de la información.
7. Dar cumplimiento a los artículos establecidos en la Ley Estatutaria N°. 1581 de 17 de octubre del 2012 por la cual se dictan disposiciones generales para la protección de datos personales.

8.3.7. Oficina De Seguridad Física

1. Elaborar y actualizar los estudios de seguridad de personal (ESP), las promesas de reserva, las pruebas técnicas de confidencialidad y/o las tarjetas de autorización para manejo de documentación clasificada, de los funcionarios que laboran en áreas donde se maneja información sensible y/o clasificada.
2. Elaborar y actualizar los estudios de seguridad de personal (ESP) y las promesas de reserva, del personal contratista y/o asesor externo que requiera interactuar con los activos de información del Hospital Militar Central.
3. 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.
4. 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.

8.3.8. Jefes De Área Y/O Unidad

1. Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

8.3.9. Dueños o Responsables De Los Activos De Información

1. 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.
2. 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.
3. Definir los requerimientos de continuidad y de recuperación en caso de desastre.
4. Coordinar un análisis de riesgos por lo menos una vez al año, para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información.

5. Comunicar sus requerimientos de seguridad de información al líder del Área de Seguridad de la Información del Hospital Militar Central.
6. Determinar y autorizar todos los privilegios de acceso a sus activos de información.
7. Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información.
8. 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.
9. 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.

8.3.10. Funcionarios, Contratistas Y Terceros

1. Cumplir con las políticas de seguridad de la información, contempladas en el presente documento.
2. Velar por el cumplimiento de las políticas de seguridad de la información dentro de su entorno laboral inmediato.
3. 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 al procedimiento de Gestión de Incidentes de Seguridad de la Información.
4. Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
5. Utilizar únicamente software y demás recursos tecnológicos autorizados.

9. IMPLEMENTACIÓN

Con el ánimo de desarrollar e implementar el sistema de gestión de seguridad de la información del Hospital Militar Central – SGSI el cual hace parte integral del sistema integrado de gestión del Hospital Militar Central, se definieron las siguientes actividades con las cuales se establece el plan de seguridad y privacidad de la información, permitiendo así la mejora continua del Sistema de Gestión de Seguridad de la Información - SGSI:

Elemento	Actividades	Tareas
Activos de la Información	Formatos y Metodología	Actualizacion de metodología y del instrumento de levantamiento de activos de la información
	Levantamiento de activos	Actualizacion de información de activos identificados
		Adición de información de activos identificados como nuevos
		Recopilar, validar y organizar activos de la infor4macion
		Clasificar los activos de la información
	Aprobar y Publicar	Presentar ante comité para aprobación los activos
		Publicar en las páginas web correspondiente.
	Definir una metodología de Análisis de riesgos	Actualización de metodología y del instrumento de análisis de riesgos de Seguridad de la Información
Valoración de los riesgos de	Identificar los riesgos	Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la

Elemento	Actividades	Tareas
seguridad de la información		continuidad de la operación de la Entidad dentro del alcance del MSPI
	Realizar un Análisis de riesgos	Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y Disponibilidad de la información que se encuentre dentro del alcance.
	Socializar los resultados al Comité de Gestión y desempeño	Presentar ante comité para aprobación
Vulnerabilidad	Análisis de Vulnerabilidades	Definir los lineamientos y alcance para pruebas de vulnerabilidades
		Desarrollar las actividades para el análisis de vulnerabilidad externos e internos
		Generar el plan de mejoramiento sobre las vulnerabilidades encontradas
Plan de Continuidad	Actualizacion del Plan de Continuidad	Actualizar el DRT – Plan de Recuperación Tecnológica Probar el Plan Mejorar el plan
Seguimiento, medición, análisis y evaluación	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI	Actualizar la Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018
		Realizar el Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.
MSPI	Integración	Integrar el MSPI con el Sistema de Gestión documental de la entidad
Indicadores	Monitoreo	Realizar el monitoreo trimestral de los indicadores definidos.
Auditorias	Auditorías Internas	Participar en las auditorías internas de seguridad de la información programadas

9.1. 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 SGSI -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

10. 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.

11. BIBLIOGRAFÍA

Señale aquí la Bibliografía consultada para la realización del presente documento utilizando las normas Apa o INCONTEC. Por favor numerarlas.

1. Consejo Nacional de Política Económica y Social (2019). Política Nacional para la Transformación Digital e Inteligencia Artificial. Bogotá, D.C.

2. Departamento Nacional de Planeación (2019). Plan Nacional de desarrollo 2018-2022: Pacto por Colombia, Pacto por la Equidad. Bogotá D.C.

3. Hospital Militar Central. Política de Seguridad de la Información (2015). Bogotá D.C.

4. Ministerio de Defensa Nacional (2017) Plan estratégico Sectorial de tecnologías de la información PETI. Bogotá D.C.

5. Ministerio de Tecnologías de la Información y Comunicaciones (2019) Manual de Gobierno Digital. Bogotá, D.C.

6. Ministerio de Tecnologías de la información y comunicaciones (2019) Modelo de Seguridad de la Información (2018). Bogotá D.C.

12. ANEXOS

https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

https://www.hospitalmilitar.gov.co/recursos_user/documentos/Planeacion_2020/Mapa-de-Procesos-2020.pdf

https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

13. 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	Actualizacion de actividades	01/03/2019
3	Actualización de Formato	Se actualiza el contenido del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualizacion contenido	Enero 2021
4	Actualización de Actividades	Actualización de: ○ Marco legal ○ Liderazgo ○ Roles y Responsabilidades ○ Actividades de Implementación	Cambios conforme a la resolución 500 de 2021	Enero de 2022

APROBACIÓN				
	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
ELABORÓ	Ingeniero Fabio Alberto Alvarado Rodríguez	Jefe Unidad de Informática	Enero de 2022	
REVISÓ	**Coronel** Ricardo Arturo Hoyos Lanziano	Subdirector de Seguridad y Defensa – Subdirección Administrativa (E)	Enero de 2022	
APROBÓ	El presente plan se encentra aprobado por el Comité Institucional de Gestión y Desempeño (*Acta de Aprobación N° 7 del 29 de diciembre de 2021*)			
PLANEACIÓN – CALIDAD Revisión Metodológica	**SMSM.** Pilar Adriana Duarte Torres	Servidor Misional de Sanidad Militar - Área Gestión de Calidad	Enero de 2022	PAT