PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL HOSPITAL MILITAR CENTRAL

MAYOR GENERAL MÉDICO
CLARA ESPERANZA GALVIS DÍAZ
DIRECTORA GENERAL
HOSPITAL MILITAR CENTRAL

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PRESENTACIÓN

El presente documento contiene el Plan de Seguridad y Privacidad de la Información del Hospital Militar Central. El cual esta 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 ko 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 esta acorde con las buenas practicas 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.

TABLA DE CONTENIDO

OBJETIVO

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.

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.

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).

POLITICA 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.

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.

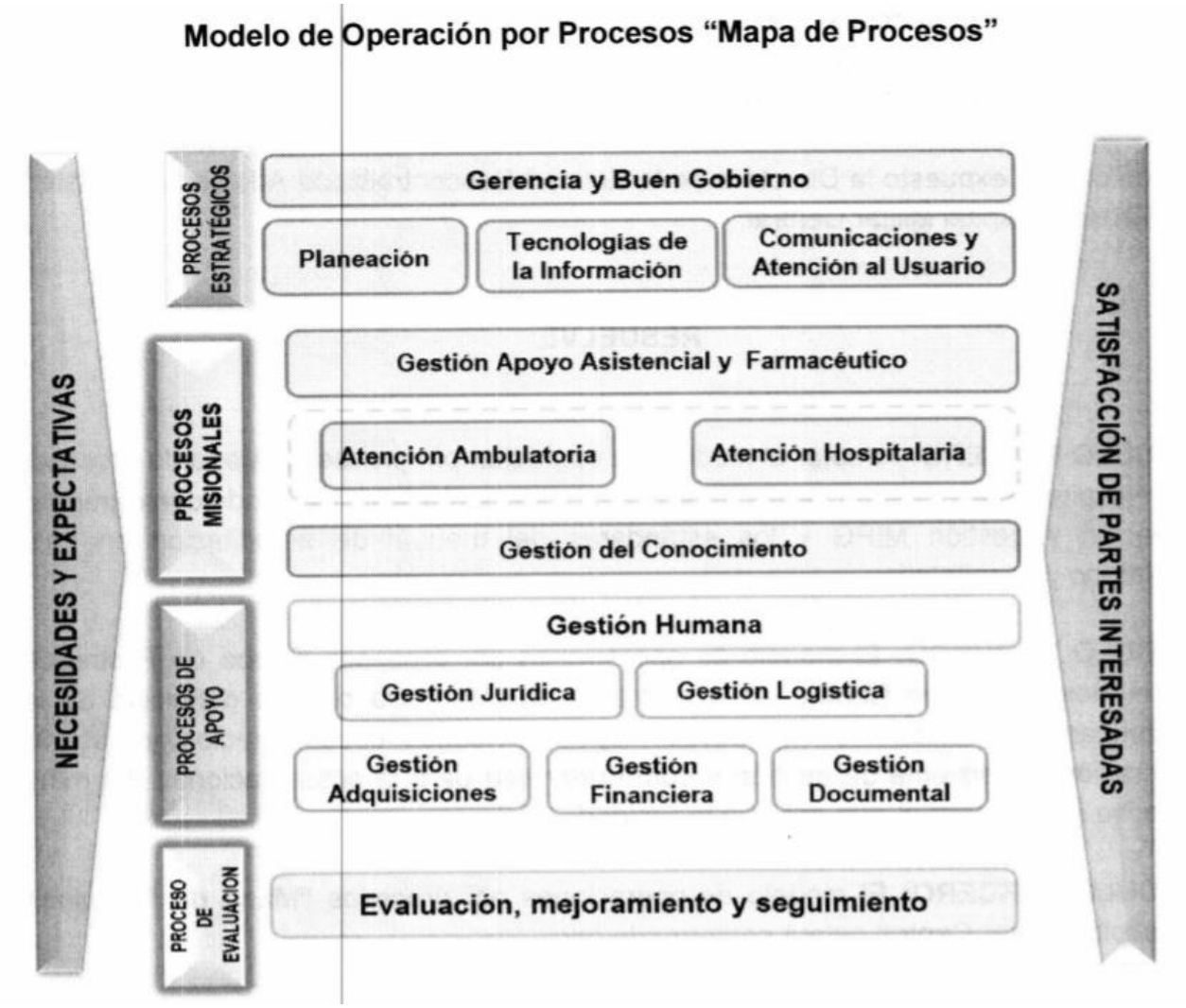
4. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

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.

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.



LIDERAZGO

La dirección General del Hospital Militar Central organizará y establecerá el comité directivo de la seguridad de la información; se deben especificar los objetivos de este comité, integrantes, deberes y responsabilidades de este, así como fijar los roles y perfiles de cada miembro del comité. Este comité debe verificar el cumplimiento de las directivas, procesos y procedimientos establecidos y generados a partir del presente plan.

ORGANIZACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La estructura del comité de seguridad de la información del Hospital Militar Central será conformada por los siguientes actores:

1. **Comité de Seguridad de la Información:** El Comité deberá estar conformado mínimo por el jefe de la Unidad de Informática, el líder del área de seguridad de la información, el Oficial de Seguridad de la información, o quien haga sus veces para cada uno de los cargos anteriormente mencionados; un representante de control interno, un representante de la oficina jurídica y un representante de la oficina de seguridad.

2. **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.

3. **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.

ROLES, RESPONSABILIDADES Y AUTORIDADES

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.

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.

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.

Oficina de Prensa Y Comunicaciones

1. Deberá divulgar la política de seguridad de la información.

Responsables de los activos de la información

1. Identificar y clasificar los activos de la información.

Usuarios, Contratistas y demás partes interesadas

1. Dar cumplimiento a lo establecido en la política de seguridad de la información
2. Informar acerca del incumplimiento de la política de seguridad de la información.

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.

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.

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.

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.

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.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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:

Planeación

A continuación, se dan a conocer las actividades definidas para en la etapa de planeación para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018 -2019, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTC-ISO-IEC 27001:2013):

ACTIVIDAD	DURACION (días)	FECHA INICIAL	FECHA FINAL
DEFINICION DEL MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	63	3/05/2018	15/02/2019
Diagnostico de Seguridad y Privacidad	13	3/05/2018	22/05/2018
Levantamiento de Informacion	5	23/05/2018	30/05/2018
Pruebas y Analisis	3	31/05/2018	5/06/2018
Informes y Recomendaciones	3	6/06/2018	11/06/2018
Diligenciamiento de la herramienta de Diagnostico del MPSI	2	12/06/2918	14/06/2018
Definicion de Roles Y Responsabilidades de Seguridad y Provacidad de la Informacion	2	15/06/2018	18/06/2018
Elaboracion de la Politica de Seguridad y Privacidad de la Informacion general	15	19/06/2018	11/07/2018
Elaboracion del Manual de políticas de seguridad y privacidad de la información	20	12/07/2018	12/07/2019
Elaboracion de Procedimientos de Seguridad de la Informacion	30	1/02/2019	31/05/2019
Definicion de los Estandares de Seguridad de la Información	30	1/02/2019	31/05/2019
Elaboracion del Plan de capacitación al interior de la entidad en Seguridad de la Informacion	8	1/11/2018	30/11/2018
Inventario de Activos de la Informacion	64	2/01/2019	31/02/2019
Identificacion de los Activos de la Informacion	20	2/01/2019	31/02/2019
determinacion de las Posibles Amenazas y Vulnerabilidades de la Arquitectura de TI	15	1/02/2019	22/02/2019
Evaluacion de los riesgos de los activos de T	15	25/02/2019	18/02/2019
Seleccionar los controles tecnicos administrativos	15	19/02/2019	15/02/2019

Implementación

A continuación, se dan a conocer las actividades definidas para en la etapa de implementación para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018 - 2019, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTCISO-IEC 27001:2013):

ACTIVIDAD	DURACION (días)	FECHA INICIAL	FECHA FINAL
IMPLEMENTACION DEL PLAN DE SEGURIDAD Y PRIVACIDAD	59	23/05/2018	5/06/2019
Elaboracion de la Declaracion de Aplicabilidad	3	4/02/2019	6/02/2019
Integracion del MPSI con el sistema de gestion documental	60	23/05/2018	23/05/2019
Elaboracion del Plan de Comunicaciones	15	1/10/2018	22/10/2018
Elaboracion Documento con la descripción de los indicadores de gestión de seguridad y Privacidad de la Informacion	8	1/03/2019	13/03/2019
Plan de Diagnostico para la Transicion de IPV4 a IPV6	30	1/04/2019	14/05/2019
Plan de implementacion de transicion de IPV4 a IPV6	15	15/05/2019	5/06/2019

Seguimiento y Mejora continua

A continuación, se dan a conocer las actividades definidas para en la etapa de seguimiento y mejora continua para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018 - 2019, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTCISO-IEC 27001:2013):

ACTIVIDAD	DURACION (días)	FECHA INICIAL	FECHA FINAL
MONITOREO Y MEJORAMIENTO CONTINUO	15	23/05/2018	16/04/2019
Elaboracion del Documento con el plan de seguimiento y revisión del MSPI	15	11/02/2019	1/03/2019
Elaboracion del Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI	15	4/03/2019	26/03/2019
Elaboracion del Documento con el plan de comunicación de resultados	15	27/03/2019	16/04/2019

MARCO LEGAL

- Ley 527 de 1999 “Comercio Electrónico”
- Ley 594 de 2000 “Ley General de Archivo”
- Ley 603 de 2000 “Control de legalidad del software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Ley 836 de 2003 “Régimen Disciplinario FF.MM”.
- Ley 1266 de 2008 “Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información”.
- Ley 1273 de 2009 “Protección de la Información y de los Datos”.
- Documento CONPES 3701 de julio del 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.

- Reglamento Interno de Trabajo
- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril 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 14 de Junio de 2018, Por el
- Y las demás normas vigentes aplicables.

REQUISITOS TECNICOS

- Modelo de Privacidad y Seguridad de la información del MINTIC.
- Norma Técnica Colombiana NTC – ISO/IEC 27000:2016

DOCUMENTOS ASOCIADOS

- Política de seguridad y Privacidad de la Información
- Directiva de control de acceso
- Plan de Sensibilización de Seguridad de la Información
- Directiva de Backup
- Directiva de Uso apropiado de correo electrónico
- Política de tratamiento de datos personales
- Directiva de reuniones

RESPONSABLE DEL DOCUMENTO

Jefe Unidad de Informática
Coordinador Área Gestión de Seguridad de la Información

Teniente **Coronel Ariadna Ramirez Ospina**
Jefe de Unidad de Seguridad y Defensa
Unidad de Informatica