PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2021

UNIDAD DE INFORMÁTICA

HOSPITAL MILITAR CENTRAL – HOMIL

CODIGO: GT-UNIN-PL-04_V01
FECHA: 13-01-2021

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se basa en una orientación estratégica y la aplicación de los lineamientos planteados en la política de administración del riesgo para el Hospital Militar Central, que requiere el planeamiento de acciones que reduzcan la afectación a la entidad en caso de materialización. De manera adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos estratégicos diseñados.

2 OBJETIVOS

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, alineados con las políticas de seguridad y privacidad de la información de la entidad y protegiendo, preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

2.1. OBJETIVOS ESPECIFICOS

- Gestionar los riesgos identificados que puedan afectar la seguridad de la información para tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos de la información a proteger en el Hospital Militar Central
- Identificar las principales amenazas que afectan a los activos de la información.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información.

3 ALCANCE

El presente plan de tratamiento de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información identificados en el Hospital Militar Central en cada uno de los procesos con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

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

Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Alcance
					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 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

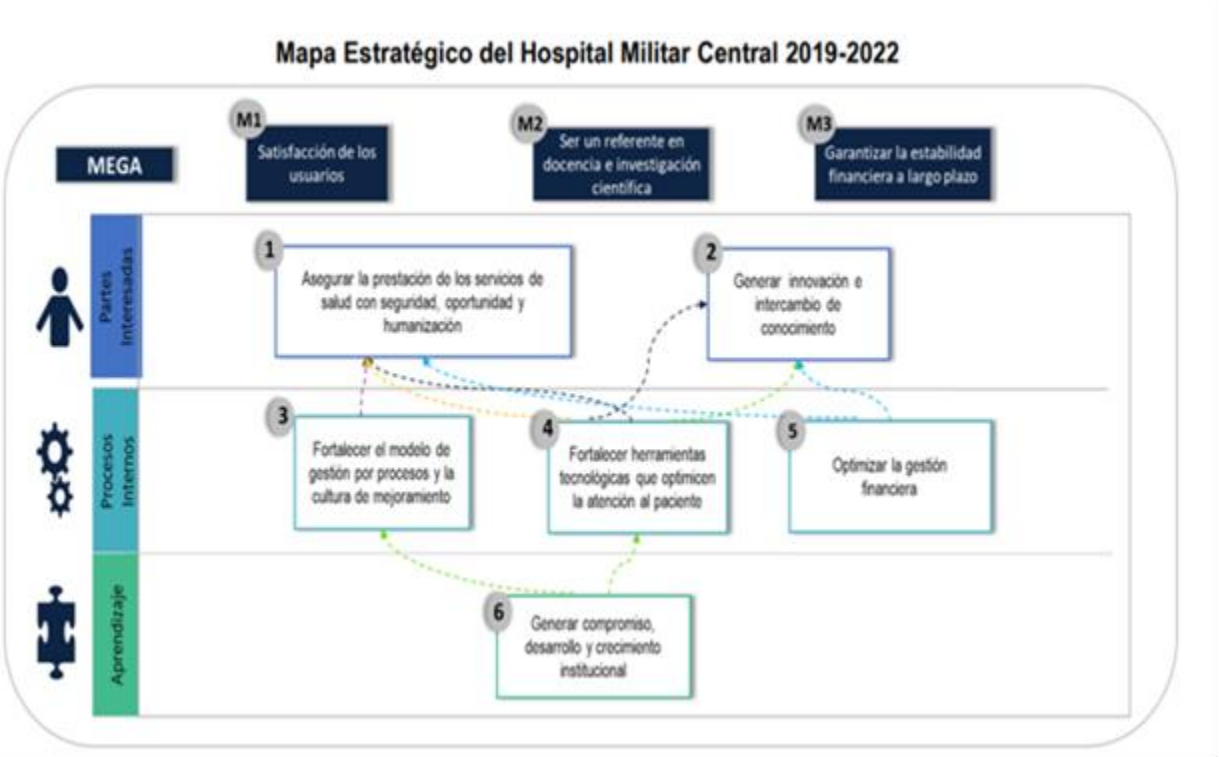
Tipo	Número	Fecha de expedición	Origen	Organismo emisor	Alcance
					Pública Nacional y se dictan otras disposiciones.
Resolución	10584	2014	Interno	Mindefensa	Por la cual se modifica parcialmente la resolución 1374 de 2012, - para ajustar las funciones del Grupo de Tecnología de Información y las Comunicaciones TIC.
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.
Política	PL-OAPL-PO-01	2020	Interna	Homil	Política de operación para la administración del riesgo en el Hospital Militar Central

5 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 (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

El Plan de Tratamiento de Riesgos de Seguridad 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 y el manejo de la seguridad de la información que se maneja a través de esos elementos.



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).

7.2. PLAN DE TRATAMIENTO DE RIESGOS

Con el ánimo de asegurar el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información - SGSI, prevenir y reducir los efectos indeseados a la hora de materializarse un riesgo que afecte un activo de la información, procurar la mejora continua, definir acciones para tratar los riesgos de seguridad de la información y evaluar la eficacia de las acciones tomadas; el Hospital Militar Central identificará y clasificará los activos de la información, identificará los riesgos de seguridad de la información y definirá las acciones a tomar bajo las siguientes premisas:

7.3. PROCESO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

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

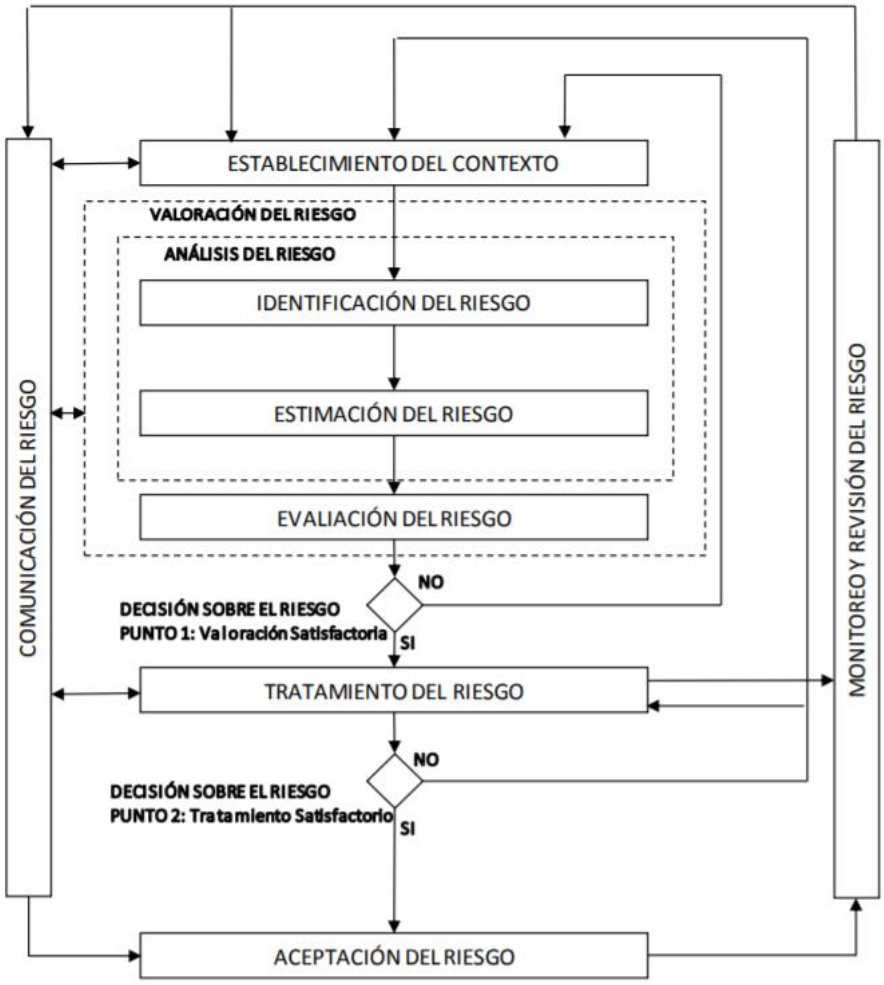
- **Información:** Información almacenada o procesada física o digitalmente " Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para 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.

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

1. Identificación o etiquetado
2. Proceso al que corresponde
3. Descripción del activo
4. Tipo de activo
5. Contenedor
6. Responsable

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

7.4. PROCESO DE VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN



Tomado de: Norma ISO/IEC 27001:2013

El análisis de riesgos se realizará todos y cada uno de los procesos procesos estratégicos, misionales, de apoyo y de evaluación del Hospital Militar Central. Los riesgos asociados a la seguridad de la información que se identifiquen a los activos de la información identificados deberán ser tratados de la siguiente manera:

1. Se realizarán entrevistas con los responsables de los activos con el fin de dar a conocer la metodología y hacer la valoración de los diferentes riesgos en términos de probabilidad e impacto.
2. Realizar el Análisis y evaluación de los riesgos de seguridad de la información para todos los activos de la información.
3. Se realizará la Identificación de opciones de tratamiento de riesgos.

4. Se realizará de manera formal una reunión para la comunicación de resultados al Comité de Seguridad de la Información.
5. El análisis y evaluación de riesgos deberá hacerse al menos una vez al año y cada vez que ocurran cambios significativos en la estructura orgánica de las dependencias y entidades que conforman el Hospital Militar Central, en la plataforma tecnológica, en los procesos, entre otros.

7.5. CRITERIOS PARA LA VALORACION DE RIESGOS

7.5.1. Probabilidad (Frecuencia)

Criterio	Valoración	Observaciones
5	CASI SEGURO	Ocurre en la mayoría de las circunstancias
4	PROBABLE	Viabilidad de ocurrencia en la mayoría de circunstancias
3	POSIBLE	Podría ocurrir en algún momento en los últimos 2 años
2	IMPROBABLE	Podría ocurrir en algún momento en los últimos 5 años
1	RARA VEZ	No ha sucedido en el último año

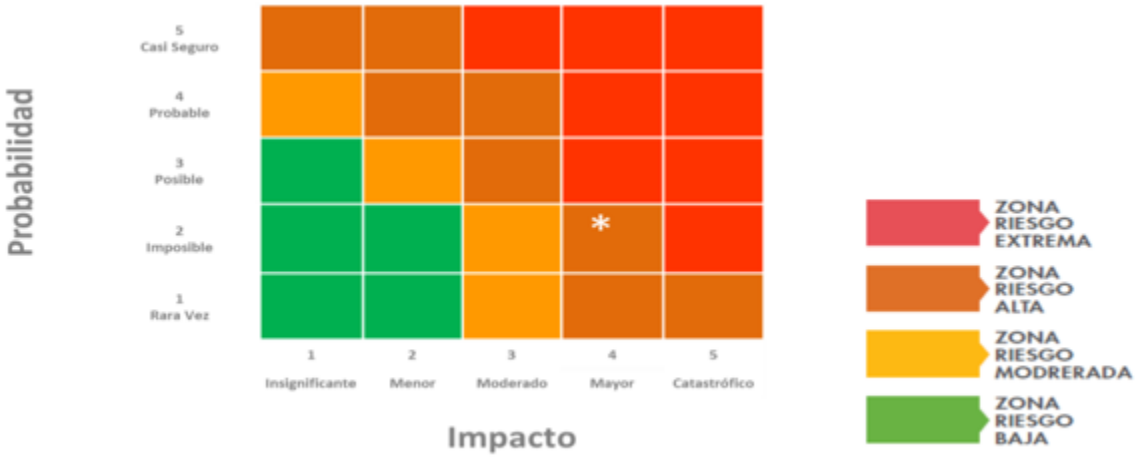
7.5.2. Impacto

Criterio	Valoración	Observaciones
5	CATASTROFICO	• Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4	MAYOR	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. •
3	MODERADO	• Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
2	MENOR	• Afectación leve de la integridad

Criterio	Valoración	Observaciones
		• Afectación leve de la disponibilidad • Afectación leve de la confidencialidad
1	INSIGNIFICANTE	• Sin afectación de la integridad • Sin afectación de la disponibilidad • Sin afectación de la confidencialidad

$$riesgo = Probabilidad * Impacto$$

VALORACION DEL RIESGO



7.6. ACCIONES PARA MITIGAR LOS RIESGOS

Resultado (de acuerdo con la Valoración)	Acción a Tomar	Observaciones
EXTREMO	EVITAR	Se deben establecer acciones de control preventivas y correctivas para evitar la materialización del riesgo
ALTO	EVITAR	Se deben establecer acciones de control preventivas para evitar la materialización del riesgo,
MODERADO	PREVENIR	Se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia
BAJO	ACEPTAR	Se debe administrar por medio de actividades propias del proceso o proyecto asociado.

La materialización de los riesgos puede ser a causa de diferentes amenazas; en el sistema de gestión de seguridad de la información del Hospital Militar Central, los riesgos de seguridad de la información serán valorados mínimo desde el punto de vista de las siguientes amenazas:

1. **De origen natural:** Fuego, inundación, desastre natural (sismo, Siniestro, meteorológico)

2. **De Origen Industrial:** Fuego, daños por agua, desastres industriales (explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tránsito), contaminación mecánica (polvo, vibraciones, suciedad), contaminación electromagnética (interferencias de radio, campos magnéticos, luz ultravioleta).
3. **Del entorno:** avería física o lógica (fallos en los equipos, fallos en los programas), corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad, Fallo en servicios de comunicaciones, interrupción de otros servicios esenciales (Papel, impresora), errores o fallos intencionados por humanos, errores del administrador, errores de configuración, deficiencias de la organización, difusión de software dañino (virus, troyanos, etc,), fugas de información, alteración accidental de la información, destrucción de la información, caída del sistema, perdida de equipos, indisponibilidad del personal.
4. **Ataques Intencionados:** Manipulación de registros, manipulación de la configuración, Suplantación de identidad, Abuso de privilegios de acceso, Uso no previsto, difusión de software dañino, errores de comunicación, acceso no autorizado, repudio, interceptación de información, modificación de la información, destrucción de la información, divulgación de la información, manipulación de programas y/o equipos, denegación de servicio, robo, ataque destructivo, ocupación enemiga, indisponibilidad del personal, ingeniería social, extorsión.

El resultado de esta fase se verá reflejado en una tabla como la siguiente:

Riesgo	Activo	Nombre del activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Valoración	Probabilidad de ocurrencia	Impacto	Opcion de Tratamiento	Controles	Eficacia	Riesgo Residual	Firma de Aceptacion Riesgo
R1													
R2													
R3													
R4													

Tabla N° 1 – Plan de Tratamiento del Riesgo

Contoles	Descripcion del Control	Aplica	Justificacion	¿Esta Implementado?	Resónsable de la aplicación	Escala de Madurez

Tabla N° 2 – Declaración de Aplicabilidad

7.7. MEDICIÓN DE LA EFICACIA

Con el fin de medir la madurez de cada control y conocer de manera adecuada la eficacia de la aplicación de uno o más controles a determinado riesgo se adopta los datos de ponderación de diseño de controles establecida así:

Calificación de controles	Ejecución	Solidez
Fuerte	Fuerte	Fuerte
	Moderado	Moderado
	Débil	Débil

Calificación de controles	Ejecución	Solidez
Moderado	Fuerte	Moderado
	Moderado	Moderado
	Débil	Débil
Debil	Fuerte	Débil
	Moderado	Débil
	Débil	Débil

A cada control se le debe dar una valoración y entendiendo que a la mitigación de un riesgo se le pueden asociar uno o varios controles mediremos la eficacia así:

$$Eficacia = \sum_{i=n}^{n} xi/n$$

Por lo anterior y teniendo en cuenta los resultados calcularemos el Riesgo Residual así:

1. Si Eficacia = 1, entonces el Riesgo Residual = Riesgo Inherente
2. Si Eficacia = 2, entonces el Riesgo Residual = Riesgo Inherente – 1 nivel valoración de riesgo
3. Si Eficacia = 3, entonces el Riesgo Residual = Riesgo Inherente – 2 niveles de valoración de riesgos

7.7.1. Aceptación de los riesgos residuales

Los responsables de los activos de la información aceptaran de manera formal los riesgos residuales y serán los responsables de realizar el inventario de activos de la información mínimo una vez al año y que se realice la adecuada valoración de riesgos de seguridad de la información

8 ROLES Y RESPONSABILIDADES

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

ROL	RESPONSABILIDADES
Comité de gestión y desempeño institucional	• Analizar los riesgos, vulnerabilidades, amenazas y escenarios de seguridad de la información que ponga en peligro el cumplimiento de objetivos estratégicos, planes institucionales, metas, compromisos en la entidad y la capacidad de prestación de servicio.
Jefe Oficina Asesora de Planeación	• Consolidar el mapa de riesgos de seguridad de la información. • Acompañar, orientar y capacitar a los lideres de procesos en la identificación, análisis, valoración y evaluación del riesgo.

ROL	RESPONSABILIDADES
Jefes de Oficina, Jefes de Unidad, Jefes de Servicio y Supervisores de Contrato	• Adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos de seguridad de la información identificados • Monitorear los riesgos identificados sobre los activos de la información y aplicar los controles definidos en los procesos a su cargo, • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión de riesgo asociado a su responsabilidad y el proceso a su cargo.
Oficina de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Realizar el seguimiento a los riesgos y a la medición del nivel de eficacia de los controles para el tratamiento de riesgos identificados en las áreas en los diferentes niveles de operación de la entidad.
Personal responsable de activos de la información	• Clasificar los activos de información bajo su responsabilidad de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad, verificar que se les proporcione un nivel adecuado de protección en conformidad con los estándares, políticas y procedimientos de seguridad de la información. • Definir los acuerdos de niveles de servicio para recuperar sus activos de información y sistemas críticos e identificar los impactos en caso de una interrupción extendida. • Definir los requerimientos de continuidad y de recuperación en caso de desastre. • 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. • Comunicar sus requerimientos de seguridad de información al líder del Área de Seguridad de la Información del Hospital Militar Central. • Determinar y autorizar todos los privilegios de acceso a sus activos de información. • Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información. • Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Estas revisiones podrán realizarse en coordinación con el custodio del activo; sin embargo, se deben verificar los resultados de las revisiones y reportar cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo

ROL	RESPONSABILIDADES
	con el procedimiento de Gestión de Incidentes de Seguridad. • Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.
Oficina de Seguridad Física	• Verificar las actividades de monitoreo del uso de los activos de información para prevenir el impacto de los riesgos derivados de pérdida de integridad, disponibilidad y confidencialidad de la información. • Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información del Hospital Militar Central.
Área de Gestión de la Seguridad de la información – Unidad de Informática	• Deberá encargarse de la planeación, control y ejecución del sistema de gestión de seguridad de la información. • Liderar el proceso de identificación y clasificación de activos de la información. • Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de la información. • Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información. • Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración. • Custodiar la información y los medios de almacenamiento bajo su responsabilidad. • Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.

9 IMPLEMENTACIÓN

Con el fin de apoyar la implementación del 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

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 la paginas web correspondiente.
		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	Verificar actividades planteadas, actualizar e incluir nuevas tareas
Protección de datos	Bases de Datos	Identificar y recolectar la información de las bases de datos con manejo de información personal
		Actualizar la información de bases de datos personales
		Implementar herramientas para anonimizar datos
Indicadores	Monitoreo	Realizar el monitoreo trimestral de los indicadores definidos.
Auditorias	Auditorías Internas	Participar en las auditorías internas de seguridad de la información programadas

10 INDICADORES

Nombre	Descripción
Cubrimiento del SGSI -Activos de la Información	Mide el cubrimiento de los activos identificados como críticos dentro de la entidad.
Apropiación de Plan de tratamiento de riesgos de seguridad de la información	Mide la apropiación de los funcionarios de la entidad en cuanto al conocimiento y desarrollo de las actividades del plan de tratamiento de seguridad de la información

11 COMUNICACIÓN Y CONSULTA

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

12 BIBLIOGRAFÍA

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.

13 ANEXOS

Omitido

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 13 de 2021

APROBACIÓN				
	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
ACTUALIZÓ	**TC.** Ariadna Ramirez Ospina	Oficial Superior en Comisión Permanente en la Administración Publica	Enero de 2021	Original Firmado
REVISÓ	**Ing.** Fabio Alvarado	Ingeniero de Sistemas Orden Prestación de Servicios – Unidad de Informática	Enero de 2021	Original Firmado
	Ing. José Miguel Cortes García	Jefe de Unidad de Seguridad y Defensa - Unidad de Informática (E)	Enero de 2021	Original Firmado
APROBÓ	El presente Plan se encuentra aprobado por el Comité Institucional de Gestión y Desempeño (***Acta de Aprobación No 01 del 26 de Enero 2021***)			
PLANEACIÓN –CALIDAD Revisión Metodológica	**SMSM.** Pilar Adriana Duarte Torres	Servidor Misional de Sanidad Militar - Área Gestión de Calidad	Enero de 2021	Original Firmado