PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Ing. Fabio Alberto Alvarado Rodríguez
Jefe de Unidad de Seguridad y Defensa
Unidad de Informática
HOSPITAL MILITAR CENTRAL - HOMIL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

El Hospital Militar Central – HOMIL, mediante la directiva permanente N° 002 del 15 de junio de 2021 “Lineamientos Para la Implementación de la Política de Gobierno Digital en el Hospital Militar Central” adoptó lo contenido en la resolución 500 de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (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". Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital. Asimismo, establece las directrices y estándares para la estrategia de seguridad digital.

Por lo anterior y teniendo en cuenta que el Modelo de Seguridad y Privacidad de la Información – MSPI indica que las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI, identificar los dueños de los riesgos, definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia, determinar el apetito de riesgos definido por la Entidad, establecer criterios de aceptación de los 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, determinar los niveles de riesgo, realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral y priorización de los riesgos analizados para su tratamiento; la entidad adoptó la Guía para la gestión de riesgos de seguridad de la información (Anexo 4. DAFP)[1] y la incluyó dentro de la Política de Operación para la Administración del riesgo en Hospital Militar Central[2] en el numeral 8.7 – Lineamientos riesgos de Seguridad de la Información

DEFINICIONES

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

OBJETIVO

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información a los que el Hospital Militar Central pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

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 resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

MARCO LEGAL

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

Tipo	Número	Fecha de expedición	Origen	Organismo Emisor	Descripción
Ley	1266	2008	Nacional	Congreso de la República	Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información
Ley	1273	2009	Nacional	Congreso de la República	Protección de la Información y de los Datos
Ley	1581	2012	Nacional	Congreso de la República	Por la cual se dictan disposiciones generales para la protección de datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013
Decreto	1377	2013	Nacional	Presidencia	por el cual se reglamenta parcialmente la Ley 1581 de 2012
Ley	1712	2014	Nacional	Congreso de la República	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Decreto	103	2015	Nacional	Congreso de la República	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto	1083	2015	Nacional	Presidencia	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital
Decreto	1078	2015	Nacional	Presidencia	Decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones

Directiva	10	2019	Nacional	Procuraduría General de la Nación	PGN Protección de Datos
Resolución	500	2021	Nacional	Min TIC	Resolución Mintic – Modelo de Seguridad y Privacidad de la Información
Resolución	746	2022	Nacional	Min TIC	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
Resolución	7870	2022	Sectorial	Min Defensa	Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades descritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.

ALINEACIÓN ESTRATÉGICA

El Plan de Tratamiento de Riesgos de Seguridad de la Información del HOMIL la Política de Operación para la Administración del riesgo en Hospital Militar Central y adopta lo establecido en la Guía para la gestión de riesgos de seguridad de la información (Anexo 4. DAFP).

ROLES Y RESPONSABILIDADES

Macro Actividad	Actividad	Tarea	Responsable	Evidencia
Gestión de riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Gestión de Seguridad Informática – GESU Oficina Asesora de planeación	Acta de Reunión
	Sensibilización	Socialización de	Gestión de	Actas de reunión,

		lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de los servicios Tecnológicos	Seguridad Informática – GESU	Grabaciones.
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Subdirectores, Jefes de oficina, Jefes de Unidad	Actas de Reunión, Grabaciones, Mapa de Riesgos
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Gestión de Seguridad Informática – GESU	Actas de Reunión, Grabaciones, Mapa de Riesgos
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Gestión de Seguridad Informática – GESU Subdirectores, Jefes de oficina, Jefes de Unidad	Actas de Reunión, Grabaciones, Mapa de Riesgos
	Publicación	Publicación mapas de riesgos en el Sitio Web	Gestión de Seguridad Informática – GESU	Mapa de Riesgos de seguridad Digital Publicado
	Seguimiento Fase de Tratamiento	Seguimiento controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Gestión de Seguridad Informática – GESU Subdirectores, Jefes de oficina, Jefes de Unidad	Seguimiento Mapa de Riesgos
	Seguimiento valoración de riesgos residuales	Seguimiento a la valoración de los riesgos residuales	Gestión de Seguridad Informática – GESU Subdirectores, Jefes de oficina, Jefes de Unidad	Seguimiento Mapa de Riesgos

	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de los planes de tratamiento y al seguimiento de la valoración de los riesgos residuales	Gestión de Seguridad Informática – GESU Subdirectores, Jefes de oficina, Jefes de Unidad	Seguimiento Mapa de Riesgos
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la Información de acuerdo con las observaciones presentadas.	Gestión de Seguridad Informática – GESU Subdirectores, Jefes de oficina, Jefes de Unidad	Seguimiento Mapa de Riesgos
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Gestión de Seguridad Informática – GESU	Seguimiento Mapa de Riesgos
Enfoque Sectorial	Acatar y Actualizar los lineamientos en seguridad y privacidad de la información emitidos por el Ministerio de Defensa Nacional	Realizar la Revisión de la resolución 7480 de 2022	Gestión de Seguridad Informática – GESU	Documentación Actualizada en el sistema de gestión de Calidad

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El Plan de Privacidad y Seguridad de la información comprende las siguientes actividades:

1. Gestión de Riesgos
    - Actualización de lineamientos de riesgos
    - Sensibilización
    - Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación
    - Aceptación de Riesgos Identificados
    - Publicación
    - Seguimiento Fase de Tratamiento

- Seguimiento valoración de riesgos residuales
- Mejoramiento
- Monitoreo y Revisión

2. Enfoque Sectorial

Actividades que se encuentran enmarcadas dentro del Plan de Seguridad y Privacidad de la información para la vigencia 2023 y fueron aprobadas por el comité de gestión y desempeño Institucional.

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.

Proceso De Valoración De Riesgos De Seguridad De La Información

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 conforme Los Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas. (2018).

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.

SEGUIMIENTO

El Plan de Tratamiento de riesgos de Seguridad de la Información es revisado y evaluado trimestralmente en la reunión general del Comité de Gestión y Seguimiento de la entidad.

COMUNICACIÓN Y CONSULTA

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

BIBLIOGRAFÍA

- Consejo Nacional de Política Económica y Social (2019). Política Nacional para la Transformación Digital e Inteligencia Artificial. Bogotá, D.C.
- Departamento Nacional de Planeación (2019). Plan Nacional de desarrollo 2018-2022: Pacto por Colombia, Pacto por la Equidad. Bogotá D.C.
- Hospital Militar Central. Política de Seguridad de la Información (2015). Bogotá D.C.
- Ministerio de Defensa Nacional (2017) Plan estratégico Sectorial de tecnologías de la información PETI. Bogotá D.C.
- Ministerio de Tecnologías de la Información y Comunicaciones (2019) Manual de Gobierno Digital. Bogotá, D.C.
- Ministerio de Tecnologías de la información y comunicaciones (2019) Modelo de Seguridad de la Información (2018). Bogotá D.C.
- [1]https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-16_Guia_administracion_riesgos_dise%C3%B1o_controles_final.pdf/fa179c5e-45bb-dffd-027c-043d4733c834?t=1609857497641
- [2]https://www.hospitalmilitar.gov.co/recursos_user/documentos/2022/PLANEACION/Poltica-de-Operacin-para-la-Administracin-del-Riesgo-en-el-HOMIL-V4-2022.pdf

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
ACTIVIDADES QUE SUFRIERON CAMBIOS		OBSERVACIONES DEL CAMBIO	MOTIVOS DE CAMBIO	FECHA DE 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	Actualización 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	Actualización contenido	Enero 2021
4	Actualización de Actividades	Según los Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas. (2018). https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b	Resolución 500 de 2021	Diciembre de 2021.
5	Actualización de Formato	Se actualiza el contenido del Plan de Seguridad y Privacidad de la Información al formato aprobado	Actualización contenido	Enero 2023

Ing. Fabio Alberto Alvarado Rodríguez
Plan de tratamiento de Riesgos de Seguridad de la información - 2023
Jefe de Unidad de Seguridad y Defensa
Unidad de Informática – Subdirección Administrativa