INFORMACIÓN GENERAL

Nombre del informe	Seguimiento a la Implementación del Modelo de Privacidad y Seguridad a los Sistemas de Información - Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información_2023
Dependencia (s)	Unidad de Informática
Auditor:	Angela Ibeth Díaz Rey

1. INTRODUCCIÓN

Dentro de las funciones señaladas en la Ley 87 de 1993 y sus decretos reglamentarios, se indica que la evaluación y el seguimiento, independiente y objetivo es uno de los roles más relevantes de la responsabilidad que le corresponde a la Oficina de Control Interno OCI, por lo cual es la encargada de la evaluación independiente del Sistema de Control Interno presentando recomendaciones y sugerencias que contribuyan a su mejoramiento y optimización de la gestión.

El ejercicio de evaluación y seguimiento, es una actividad independiente y objetiva de aseguramiento y consultoría, concebida para agregar valor y mejorar las operaciones del Hospital Militar Central; fortaleciendo el cumplimiento de sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

Es así que la Oficina de Control Interno, realizó seguimiento a la implementación del Modelo de Privacidad y Seguridad de Información; el cual busca preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, brindando confianza a las partes interesadas.

2. OBJETIVO

Hacer seguimiento al diseño e implementación del Modelo de Seguridad y Privacidad de la Información MPSI de HOMIL, de conformidad con lo establecido en la normatividad vigente, en relación al modelo de privacidad y seguridad de los sistemas de información, manuales, protocolos, políticas, planes y procedimientos, con el fin de verificar los lineamientos y directrices establecidos.

3. ALCANCE

El seguimiento de la implementación del modelo de privacidad y seguridad de los sistemas de información, se desarrolló mediante el análisis de la herramienta de MinTIC denominada Autodiagnóstico de Seguridad y Privacidad de la Información_2023, así como al cumplimiento de políticas y lineamientos emitidos por esta entidad.

4. METODOLOGÍA

La metodología utilizada se basó en el análisis de la información solicitada, donde se utilizaron diferentes técnicas así:

1. Verificación y análisis de documentos y/o registros físicos y virtuales, consulta en el Sistema de Información y en la página Web de la entidad, en cual fueron verificadas las diferentes políticas y procedimientos establecidos, así como el mapa de riesgos vigente.
2. Reuniones con el Jefe de la Unidad Informática y el Oficial de Seguridad.
3. Solicitud de información: Se solicitó información asociadas al MPSI (Modelo de Privacidad y Seguridad de la Información) y a su implementación en la entidad según los lineamientos de MinTIC(Tabla1) así:

Tabla 1 Información solicitada por la OCIN

META	ÍTEM	DOCUMENTO MPSI MINTIC
DIAGNÓSTICO	Determinar el estado actual de privacidad de la información al interior de la Entidad.	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf

META	ÍTEM	DOCUMENTO MPSI MINTIC
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf
PLANIFICACIÓN	Política de Seguridad y Privacidad de la Información.	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializado al interior de la Entidad.
	Política de Seguridad y Privacidad de la Información.	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.
	Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
	Roles y responsabilidades para la seguridad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.
	Inventario de Activos de Información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.
		Matriz con la identificación, valoración y clasificación de activos de Información.

META	ÍTEM	DOCUMENTO MPSI MINTIC
		Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6
	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.
	Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos.
		Documento con el análisis y evaluación de riesgos.
		Documento con el plan de tratamiento de riesgos.
		Documento con la declaración de aplicabilidad.
		Documentos revisados y aprobados por la alta dirección.
	Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
	Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.
IMPLEMENTACIÓN	Planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
	Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
	Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
	Plan de Transición de IPv4 a IPv6.	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.
EVALUACIÓN DE DESEMPEÑO	Plan de seguimiento, evaluación y análisis del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta dirección.
	Plan de Ejecución de Auditorías	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

META	ÍTEM	DOCUMENTO MPSI MINTIC
MEJORA CONTINUA	Plan de mejora continua	Documento con el plan de mejoramiento.
		Documento con el plan de comunicación de resultados.

FUENTE: Modelo de Seguridad y Privacidad de la Información – MINTIC

5. CRITERIO LEGAL

- Constitución Política de Colombia. Los Artículos 15, 209 y 269 definen el derecho a la intimidad y al buen nombre.
- NTC / ISO 27001 2013 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
- NTC / ISO 27002 2013 Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
- Ley 1712 de 2014. 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 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Documento técnico externo 2016, Modelo de Seguridad y Privacidad de la Información – MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Versión 3.0.2, julio de 2016.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Resolución 1519 de 2020 Ministerio de Tecnologías de la Información y las Comunicaciones, Define los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014.
- Resolución 500 Anexo 1 Nuevo MSPI 2021, Por medio del cual el Ministerio de TIC actualiza el Modelo de Seguridad y Privacidad de la Información – MSPI.

- Resolución MinTIC 746 del 11 marzo de 2022, 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 de 2022 Ministerio de Defensa.
- Directiva Presidencial 002 de 2022 Reiteración de la política pública en materia de seguridad digital.
- CONPES 3701 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3995 2020 Política Nacional de Confianza y Seguridad Digital.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- Procedimiento: Gestión para la Elaboración e Implementación de la Política de Seguridad de la Información – GT- GESU-PR-01 V2.
- Circular 01 de 2022 Presidencia de la República.
- Directiva 02 de 2022 Presidencia de la República.
- Procedimiento: Inventario y Clasificación de Activos de la Información GT-UNIN-PR-06 V2-MinTIC.
- Plan de Seguimiento, Evaluación y Análisis del MSPI GT-SEGU-PL-01 V1 MinTIC.
- Plan de Sensibilidad y Capacitación en Seguridad de la Información GT-UNIN-PL-06 V1 MinTIC.
- Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2 MinTIC.
- Documento Informativo Para la Gestión de Incidentes de Seguridad de la Información - GT-GERE-PR-01-DI-01_V1 MinTIC.
- Roles y Responsabilidades Para la Seguridad Digital y el Modelo de Privacidad y Seguridad de la Información del HOMIL - GT-UNIN-PL-05-DI-02 V1 MinTIC.
- Política General de Seguridad y Privacidad de la Información - GT-UNIN-PO-01 V1 MinTIC.

6. RESULTADOS DEL SEGUIMIENTO

Durante el seguimiento al Modelo de Seguridad y Privacidad de la Información del HOMIL, por parte de la Oficina de Control Interno se verificó que, desde la elaboración del Diagnóstico, así como del Plan de Trabajo, y la permanente actualización y mejora de los documentos e instrumentos que se desprenden del Modelo, han sido elaborados y actualizados siguiendo las directrices del MINTIC.

El Hospital Militar Central – HOMIL, adoptó mediante la directiva permanente N° 002 del 15 de junio de 2021 "Lineamientos Para la Implementación de la Política de Gobierno Digital en el Hospital Militar Central"; a fin de alinear su Plan de Seguridad y Privacidad de la Información con las resoluciones 500 de 2021 y

746 de 2022, expedidas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC y al Modelo de Privacidad y Seguridad de la Información de la entidad alineado al Plan de seguridad y privacidad de la información del Sector Defensa.

6.1 AVANCE DEL MPSI EN HOMIL

6.1.1 Contexto:

El MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y definió los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), teniendo en cuenta lo anterior y de acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información_2023, realizado por la Unidad de Informática en HOMIL, en la Tabla 2, se muestra el avance del PHVA que se encuentra en un 94%, para el Hospital, así:

Tabla 2 Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA)

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	37%	40%
Implementación	19%	20%
Evaluación de desempeño	20%	20%
Mejora continua	18%	20%
TOTAL	**94%**	**100%**

Fuente: Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información_2023 - Unidad de Informática

6.1.1.1 Fase de Planificación:

En esta fase se obtuvo una puntuación del 37%, del máximo evaluado por MinTIC que es del 40%, la OCIN estableció que de los ítems evaluados HOMIL cumple con:

a. Alcance MSPI.
b. Acto administrativo con las funciones de seguridad y privacidad de la información.
c. Política de seguridad y privacidad de la información.
d. Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.
e. Procedimiento de inventario y Clasificación de la Información e infraestructura crítica.
f. Metodología de inventario y clasificación de la información e infraestructura crítica.
g. Procedimiento de gestión de riesgos de seguridad de la información.
h. Plan de tratamiento de riesgos de seguridad de la información.
i. Declaración de aplicabilidad.
j. Manual de políticas de Seguridad de la Información.
k. Plan de capacitación, sensibilización y comunicación de seguridad de la información.

No obstante, la puntuación obtenida se debe al literal K), dado que de lo solicitado por MinTIC, la OCIN no evidenció:

a. Elaboración de folletos y boletines.
b. Medición de sensibilización realizada a nuevos empleados y contratistas.
c. La inclusión en los temas de toma de conciencia, los procedimientos como reporte de incidentes de seguridad de la información.
d. Encuestas para establecer si funcionarios con roles privilegiados entienden sus responsabilidades y roles.

6.1.1.2 Fase de Implementación:

En esta fase la entidad obtuvo una puntuación de 19% del 20%, dado que de acuerdo con los instrumentos de medición del MinTIC, el Modelo de Seguridad y Privacidad de la Información - MSPI, esta fase contempla 6 niveles de madurez, los cuales permiten identificar los niveles de evaluación aplicados a la seguridad de la información: Inexistente, Inicial, Repetible, Efectivo, Gestionado y Optimizado, en la Tabla 3 Evaluación de Efectividad de Controles, se muestra el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013:

Tabla 3 Evaluación de Efectividad de Controles

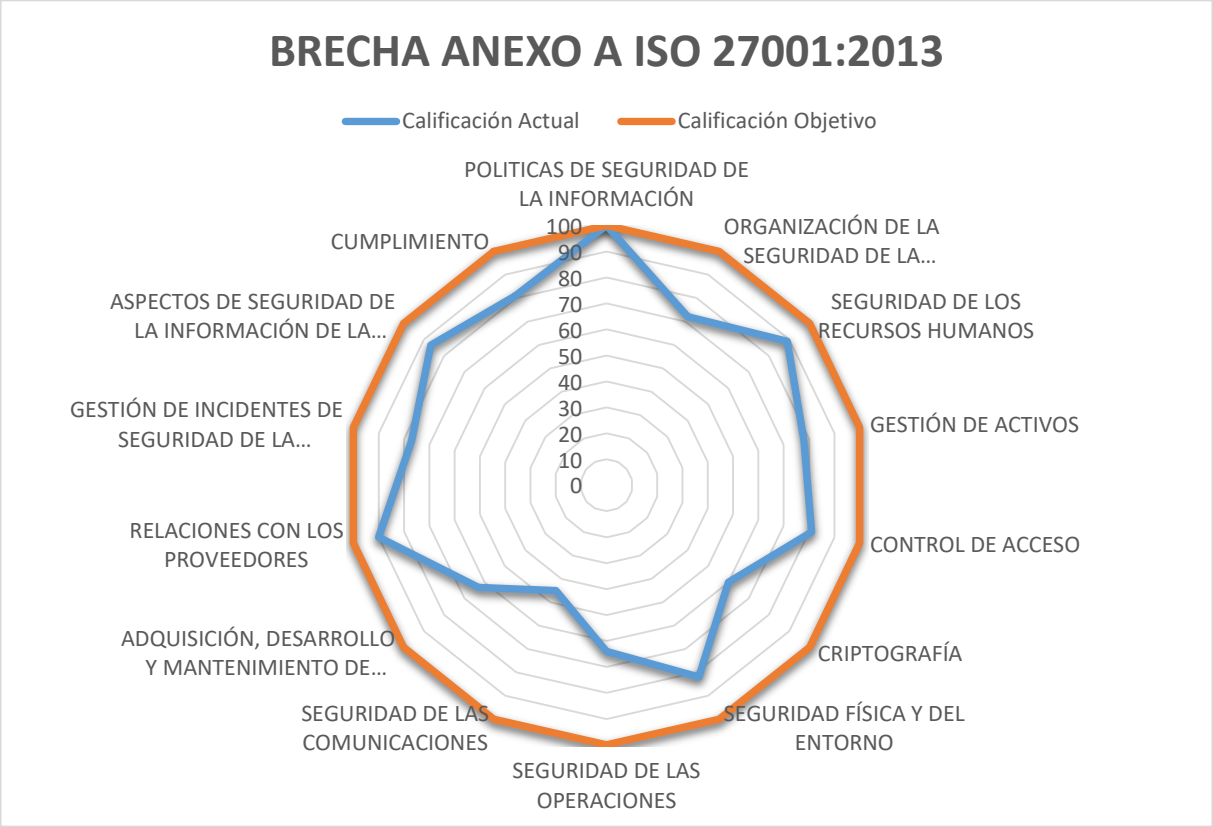
ISO No.	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	Políticas de seguridad de la información	100	100	OPTIMIZADO
A.6	Organización de la seguridad de la información	72	100	GESTIONADO
A.7	Seguridad de los recursos humanos	89	100	OPTIMIZADO
A.8	Gestión de activos	78	100	GESTIONADO
A.9	Control de acceso	81	100	OPTIMIZADO
A.10	Criptografía	60	100	EFECTIVO
A.11	Seguridad física y del entorno	82	100	OPTIMIZADO
A.12	Seguridad de las operaciones	64	100	GESTIONADO
A.13	Seguridad de las comunicaciones	45	100	EFECTIVO
A.14	Adquisición, desarrollo y mantenimiento de sistemas	63	100	GESTIONADO
A.15	Relaciones con los proveedores	90	100	OPTIMIZADO
A.16	Gestión de incidentes de seguridad de la información	77	100	GESTIONADO
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	87	100	OPTIMIZADO
A.18	Cumplimiento	81	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**76**	**100**	GESTIONADO

Fuente: Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información_2023 - Unidad de Informática

Conforme al análisis y los resultados obtenidos, la puntuación promedio de los controles de la entidad fue de 76%, por lo cual la entidad se halla en un proceso "Gestionado" de medidas para la seguridad y

privacidad de la información, en la ilustración 1, se presenta la brecha que tiene HOMIL con respecto a la calificación objetivo de la norma ISO 27001:2013.

Ilustración 1 Brecha de la evaluación de HOMIL respecto a la Calificación objetivo de la ISO 27001:2013



Fuente: Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información_2023 - Unidad

Teniendo en cuenta que el objetivo es lograr el 100% en la implementación del modelo de seguridad y privacidad de la información MPSI y que la entidad se encuentra en la etapa de mejora continua del modelo PHVA, la OCIN pudo evidenciar que existe una oportunidad de mejora en diversos aspectos de la gestión de la seguridad de la información entre los cuales se destacan los controles con calificación más baja que lo cales son A.13 Seguridad de las comunicaciones puntuación del 45%, A.10 Criptografía puntuación del 60%, Adquisición, desarrollo y mantenimiento de sistemas puntuación 63% y Seguridad de las comunicaciones con 64%.

6.1.1.2.1 A.13 Seguridad de las comunicaciones

Para este numeral la Oficina de Control Interno evidenció en el archivo de Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información_2023, enviado por la Unidad de Informática, que fue evaluado lo solicitado por MinTIC, en cuanto a:

A.13.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**
A.13.1.1	Controles de redes
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Separación en las redes
A.13.2	**TRANSFERENCIA DE INFORMACIÓN**
A.13.2.1	Políticas y procedimientos de transferencia de información
A.13.2.2	Acuerdos sobre transferencia de información
A.13.2.3	Mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o de no divulgación

De acuerdo a lo anterior, la OCIN evidenció que el punto A.13.1 Gestión de Seguridad de redes se encuentra inmerso en: el manual de políticas de seguridad de la información, el PROCEDIMIENTO: GESTIÓN TECNOLÓGICA - INCO CÓDIGO: GT-INCO-PR-02, el formato Único de Solicitud de Acceso a las Tecnologías de la Información Cód.: IM-UNIN-FT-02, y el formato COMPROMISO DEL USUARIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN GT-UNIN-PR-04-FT-02; del numeral A.13.2 Transferencia de información no se evidenció su inclusión en el sistema documental institucional HOMIL, políticas y/o procedimientos de transferencia de información y mensajería electrónica, así mismo, en el PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (2023 -2026) de la UNIDAD DE INFORMÁTICA, CÓDIGO: GT-UNIN-PL-03, VERSIÓN: 01, de fecha de emisión 29-01-2024, se evidenció que no quedó algo específico sobre el tratamiento del ítem A.13 Seguridad de las comunicaciones de la norma ISO 27001:2013.

6.1.1.2.2 A.10 Criptografía

En el archivo de Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información_2023 la Unidad de Informática evaluó:

A.10.1	**CONTROLES CRIPTOGRÁFICOS**

A.10.1.1 Política sobre el uso de controles criptográficos

A.10.1.2 Gestión de llaves

La OCIN pudo evidenciar que en el MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CÓDIGO: GT-UNIN-MN-03 en el punto 6.13 CONTROLES CRIPTOGRÁFICOS, se especifica el responsable que debe identificar definir e implementar los mecanismos y controles criptográficos, ver Ilustración 2, pero no se plantea lo solicitado en el anexo 1 de la resolución 500 del 2021 de MinTIC, debido a que no se ha establecido la política sobre el uso de controles criptográficos ni gestión de llaves.

Ilustración 2 Manual de lineamientos de seguridad y privacidad de la información

MANUAL	MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CODIGO	GT-UNIN-MN-03	VERSION	02
		Página:		14 de 39	

6. LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4. Es deber de cualquier funcionario, contratista y/o tercero reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

Las características de las contraseñas empleadas en la infraestructura tecnológica deben cumplir los requerimientos definidos en el procedimiento de Gestión de Usuarios y Contraseñas.

6.13. CONTROLES CRIPTOGRÁFICOS – Ref.: ISO/IEC 27001: 2013 CL. A.10.1

a. La Unidad de Informática, debe identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en el procedimiento de Inventario y Clasificación de Activos de Información, tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

b. No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la Unidad de Informática, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios, contratistas y demás terceros autorizados.

c. Realizar una gestión adecuada de las claves mediante procesos seguros para la creación, manipulación y destrucción de las claves criptográficas.

d. Llevar un registro y auditoría de las actividades relacionadas con la gestión de las claves criptográficas.

6.14. SEGURIDAD FÍSICA Y DEL ENTORNO – Ref.: ISO/IEC 27001:2013 CL. A.11.1.1, CL. A.11.1.3, CL A.11.1.4.

a. La protección física se lleva a cabo mediante la creación de diversas barreras o medidas de control físicas, alrededor de las instalaciones del Hospital Militar Central.

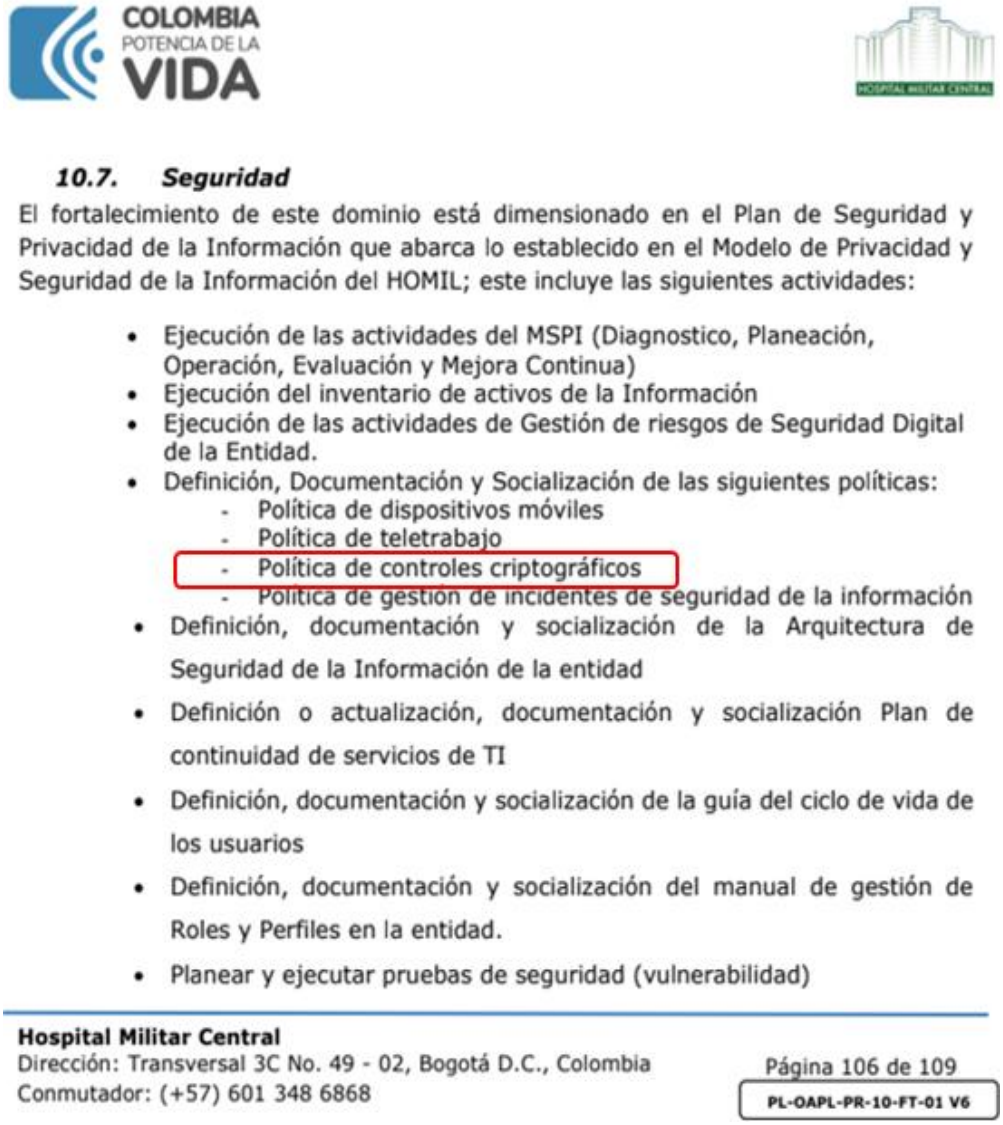
b. Las áreas protegidas se resguardan mediante el empleo de controles de acceso físico, los que serán determinados por el oficial de seguridad de la información, a fin de permitir el acceso solo a personal autorizado.

c. Para la selección de las áreas protegidas se tiene en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se toma en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

Fuente Sistema documental HOMIL

Así mismo, se evidenció que en el PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (2023 - 2026), de la UNIDAD DE INFORMÁTICA, CÓDIGO: GT-UNIN-PL-03, VERSIÓN: 01, de fecha de emisión 29-01-2024 en la página 106, (Ilustración 3 Plan Estratégico de Tecnologías de la Información (2023 -2026), en el numeral 10. Situación Objetivo (TO – BE) (…) 10.7. Seguridad, se plantea la definición, documentación y socialización de la política de controles criptográficos, como se presenta a continuación:

Ilustración 3 Plan Estratégico de Tecnologías de la Información (2023 -2026)



10.7. Seguridad

El fortalecimiento de este dominio está dimensionado en el Plan de Seguridad y Privacidad de la Información que abarca lo establecido en el Modelo de Privacidad y Seguridad de la Información del HOMIL; este incluye las siguientes actividades:

- Ejecución de las actividades del MSPI (Diagnostico, Planeación, Operación, Evaluación y Mejora Continua)
- Ejecución del inventario de activos de la Información
- Ejecución de las actividades de Gestión de riesgos de Seguridad Digital de la Entidad.
- Definición, Documentación y Socialización de las siguientes políticas:
  - Política de dispositivos móviles
  - Política de teletrabajo
  - Política de controles criptográficos
  - Política de gestión de incidentes de seguridad de la información
- Definición, documentación y socialización de la Arquitectura de Seguridad de la Información de la entidad
- Definición o actualización, documentación y socialización Plan de continuidad de servicios de TI
- Definición, documentación y socialización de la guía del ciclo de vida de los usuarios
- Definición, documentación y socialización del manual de gestión de Roles y Perfiles en la entidad.
- Planear y ejecutar pruebas de seguridad (vulnerabilidad)

Hospital Militar Central
Dirección: Transversal 3C No. 49 - 02, Bogotá D.C., Colombia
Conmutador: (+57) 601 348 6868

Página 106 de 109
PL-OAPL-PR-10-FT-01 V6

Fuente Sistema documental HOMIL

No obstante, lo anterior, la puntuación obtenida obedece a que la entidad no cuenta con la Política sobre el uso de controles criptográficos y gestión de llaves.

6.1.1.2.3 A.14 Adquisición, desarrollo y mantenimiento de sistemas

En el archivo de Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información_2023 la Unidad de Informática evaluó:

A.14.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones
A.14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**
A.14.2.1	Política de desarrollo seguro
A.14.2.2	Procedimientos de control de cambios en sistemas
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
A.14.2.4	Restricciones en los cambios a los paquetes de software
A.14.2.5	Principios de construcción de sistemas seguros
A.14.2.6	Ambiente de desarrollo seguro
A.14.2.7	Desarrollo contratado externamente
A.14.2.8	Pruebas de seguridad de sistemas
A.14.2.9	Prueba de aceptación de sistemas
A.14.3	**DATOS DE PRUEBA**
A.14.3.1	Protección de datos de prueba

La Oficina de Control Interno evidenció que el punto A.14.1 está incluido dentro de MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CÓDIGO: GT-UNIN-MN-03, aunque los puntos A14.2 y A14.3, no cuenta con los requisitos de documentación requeridos en los mismos, y no se encuentran incluidos dentro del PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (2023 - 2026), de la UNIDAD DE INFORMÁTICA, CÓDIGO: GT-UNIN-PL-03, VERSIÓN: 01.

6.1.1.2.4 A.12 SEGURIDAD DE LAS OPERACIONES

En el archivo de Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información_2023, la Unidad de Informática evaluó:

A.12.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**
A.12.1.1	Procedimientos de operación documentados
A.12.1.2	Gestión de cambios
A.12.1.3	Gestión de capacidad
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
A.12.2	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**
A.12.2.1	Controles contra códigos maliciosos
A.12.3	**COPIAS DE RESPALDO**
A.12.3.1	Respaldo de la información
A.12.4	**REGISTRO Y SEGUIMIENTO**
A.12.4.1	Registro de eventos
A.12.4.2	Protección de la información de registro
A.12.4.3	Registros del administrador y del operador
A.12.4.4	Sincronización de relojes
A.12.5	**CONTROL DE SOFTWARE OPERACIONAL**
A.12.5.1	Instalación de software en sistemas operativos
A.12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA
A.12.6.1	Gestión de las vulnerabilidades técnicas
A.12.6.2	Restricciones sobre la instalación de software
A.12.7	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**
A.12.7.1	Controles sobre auditorías de sistemas de información

La OCIN evidenció que se utilizan los documentos PROCEDIMIENTO: GESTIÓN TECNOLÓGICA -INCO CÓDIGO: GT-INCO-PR-02 y PROCEDIMIENTO: ADMINISTRACIÓN DE BASES DE DATOS CÓDIGO: GT-UNIN-PR-02, sin embargo no hay procedimientos operativos documentados, con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores,

contactos de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

En el caso del numeral A.12.2.1 de acuerdo a lo establecido por MNTIC no se evidenció documentada la política que prohíba el uso de software no autorizado por HOMIL.

6.1.1.3 Fase de Evaluación de Desempeño:

Dentro de esta fase se determina el sistema y forma de evaluación de la adopción del modelo, la OCIN identificó que el HOMIL cuenta con un plan de auditorías y un plan de seguimiento para el seguimiento de la evaluación del MPSI, liderada por el Oficial de Seguridad de la información de la entidad.

6.1.1.4 Fase de Mejora Continúa:

Dentro de esta fase de del MPSI se debe establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición, la OCIN pudo identificar que HOMIL cuenta con el plan de mejoramiento y el plan para la comunicación de resultados de la gestión e implementación del MSPI, informe que la Unidad de Informática por medio de la herramienta de autogestión viene haciendo anualmente.

Por lo anteriormente expuesto, la Oficina de Control Interno identificó lo siguiente:

6.1.2 Condición:

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información_2023 efectuado por la Unidad de Informática de HOMIL, de la Política Nacional de Gobierno Digital, en la "Tabla 2 Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA) en la Fase de Implementación", se observa que el porcentaje de avance logrado por el Hospital Militar Central, corresponde a un 94%, evidenciando que la entidad se ha orientado para dar cumplimiento a los lineamientos dados por MinTIC para la implementación del modelo de seguridad y privacidad de la información.

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares

internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

6.1.3 Criterio:

- Resolución 500 de marzo 10 de 2021 "*Por medio del cual el Ministerio de TIC actualiza el Modelo de Seguridad y Privacidad de la Información – MSPI*", Anexo 1 "*MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*", numeral 11, inciso 11.1 *Controles y objetivos de control*.
- Norma NTC: ISO/IEC 27001:2013, anexo A los cuales tratan de los objetivos de control, en los numerales A.10 Criptografía, A.12 Seguridad de las Operaciones, A.13 Gestión de la Seguridad de Redes y A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas

Causa:

Debilidades en la aplicación en la Resolución 500 de marzo 10 de 2021, anexo 1 "Fase 3: Evaluación de desempeño", teniendo en cuenta que el Modelo de seguridad y Privacidad de la Información MPSI.

6.1.4 Consecuencia:

Posibles observaciones e incidencias por parte de Entes de Control.

6.1.5 Observación 1:

Un posible incumplimiento en el anexo 1 numeral 9.1.1 de la resolución 500 de MinTIC del 10 de marzo 2021 en la fase de implementación debido a que HOMIL se encuentra con calificaciones bajas y en estado "EFECTIVO" y "GESTIONADO" en la evaluación de controles ISO 27001:2013, (**Tabla 3** Evaluación de Efectividad de Controles, para el año 2023.

6.1.6 Recomendación 1

Analizar la pertinencia de elaborar las políticas y/o procedimientos de Criptografía, Seguridad de las Operaciones, Seguridad de las comunicaciones y Adquisición de desarrollo y mantenimiento de sistemas,

según lo solicitado por MinTIC en la resolución 500 y su anexo 1, teniendo en cuenta la norma ISO27001:2023.

6.1.7 Recomendación 2

Continuar avanzado con el cumplimiento en cuanto a la inclusión de las política y procedimientos necesarios para subir la calificación de evaluación de implementación del modelo MPSI, en su fase evaluación del desempeño del modelo PHVA, según lo planteado en este informe, dentro PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (2023 -2026), de la UNIDAD DE INFORMÁTICA, CÓDIGO: GT-UNIN-PL-03, VERSIÓN: 01.

6.2. RESPONSABLE MPSI

6.2.1. Condición

El Hospital militar dando cumplimiento al numeral "*11.2 Guía - Roles y responsabilidades*" del anexo 1 de la resolución 0500 del 2021, definió en el plan de seguridad y privacidad de la información, código GT-UNIN-PL-04, versión: 01 de fecha 29-01-2024, en el numeral 8 los "Roles y Responsabilidades de Seguridad de la Información", requeridos en el MSPI, que plantea un equipo conformado por los siguientes roles:

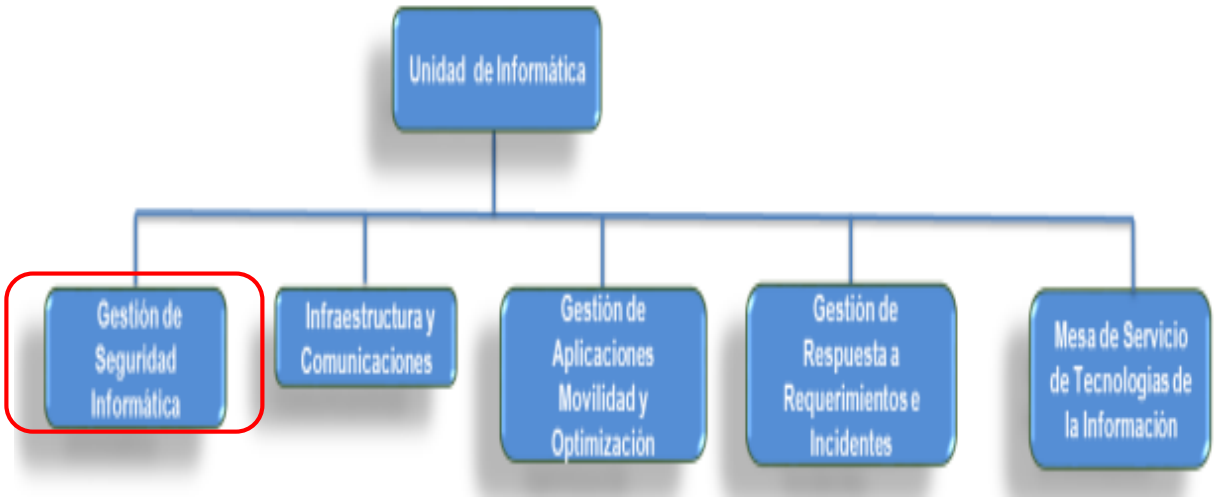
Tabla 4 Roles

No.	ROL
1	Comité de Gestión y Desempeño
2	Unidad de Informática
3	Oficial de Seguridad Digital
4	Talento Humano
5	Unidad de Compras, Licitaciones y bienes Activos
6	Oficina de Control Interno
7	Comunicaciones y Relaciones Públicas
8	Oficina Asesora Jurídica
9	Área de Seguridad Física
10	Todos los funcionarios y contratistas

FUENTE: Unidad Informática HOMIL

Ahora bien, La OCIN de acuerdo con la información suministrada identificó que la Unidad de Informática definió su estructura jerárquica así:

Ilustración 4 Organigrama Unidad Informática



Fuente Unidad Informática HOMIL

En el presente seguimiento, la OCIN estableció que está creado el grupo Gestión de Seguridad Informática, no obstante, teniendo en cuenta las directrices emitidas por MinTIC en la resolución 0500 de 2021, este rol debe ser independiente de la Unidad Informática, también, se identificó que se contrató por OPS al oficial de seguridad de la información en línea con lo señalado en el MPSI así:

Tabla 5 Comparativo perfil Oficial de Seguridad de la Información

PERFIL MPSI MINTIC	OFICIAL DE SEGURIDAD HOMIL
Profesional en el área de sistemas, informática o carreras afines.	Ingeniero en Telecomunicaciones 2021.
Experiencia mínima de 2 años en cargos relacionados con la seguridad informática.	Hospital Militar Central 2018 a la fecha.

PERFIL MPSI MINTIC	OFICIAL DE SEGURIDAD HOMIL
Conocimientos en normativas de seguridad de la información, tales como ISO 27001, NIST, entre otras.	• Gestión de la Seguridad de la Información Auditor Interno en la norma ISO/IEC 27001:2022. • Hacking Ético: Offensive and Defensive 3.0 (HE-OF&DF 3.0). • Certificación Fortinet NSE 1 Network Security Associate. • Microsoft Cybersecurity Architect (SC-100T00-A). • Designing and Implementing a Microsoft Azure AI Solution (AI-102T00-A). • Microsoft Azure Fundamentals (AZ-900T00-A).
Experiencia en la implementación y gestión de controles de seguridad informática en infraestructuras tecnológicas.	Hospital Militar Central 2018 a la fecha.
Capacidad para realizar análisis de vulnerabilidades, evaluación de riesgos y elaboración de planes de respuesta a incidentes de seguridad.	Hospital Militar Central 2018 a la fecha.
Experiencia en la administración de sistemas de protección contra intrusiones, firewalls y sistemas de detección de malware.	Hospital Militar Central 2018 a la fecha.
Habilidades para la comunicación efectiva con diferentes stakeholders y para la elaboración de informes técnicos.	Hospital Militar Central 2018 a la fecha.
Certificaciones en seguridad informática como CompTIA Security+, CISSP, CISA u otras serán valoradas positivamente.	Especialización en Seguridad Informática - Fundación Universitaria San Mateo.
Aptitudes para trabajar en equipo, proactivo, autónomo y con capacidad para resolver problemas de forma eficiente.	Hospital Militar Central 2018 a la fecha.

FUENTE: Elaboración propia con información del perfil MPSI de MINTIC y hoja de vida del Oficial de Seguridad del HOMIL

6.2.2 Criterio:

Resolución 500 del 10 de marzo de 2021 de MinTIC, donde se establece en el "***ARTÍCULO 6o. LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y LA GESTIÓN DE RIESGOS DE LA ENTIDAD (…)*** ***numeral*** *9.Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información****."*

Así mismo, en el anexo 1 (Ilustración 5), de esta resolución quedó explícito en el numeral 7.2.3:

Ilustración 5 Resolución 0500 del 2021

7.2.3 Roles y responsabilidades

Lineamiento: Articular con las áreas o dependencias de la Entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la Entidad.

Se debe delegar a un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; si el cargo no existe en la Entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz.

Propósito: Hay que asegurar que los funcionarios de la Entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

Entradas recomendadas	Salidas
- 7.1.3 Definición del alcance del Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. - ¡Error! No se encuentra el origen de la referencia.	Roles y responsadilidades

Fuente MinTIC

6.2.3 Causa:

Posible desconocimiento en el responsable de la seguridad y privacidad de la información, debido a que este rol no debe depender de la Unidad Informática y debe ser delegada por acto administrativo.

6.2.4 Consecuencia:

Posibles hallazgos por entes de control.

6.2.5 Recomendación 3

Nota: Teniendo en cuenta el seguimiento realizado en el año 2023, relacionado con la Implementación del Modelo de Privacidad de la Información MPSI, donde se formuló un hallazgo el cual cita: "*La OCIN evidenció incumplimiento del numeral 8.2.2 correspondiente a lo estipulado en el Plan de Privacidad y Seguridad de la Información; donde hace referencia al cargo de Oficial o Promotor de la Seguridad y Privacidad de la Información; el cual será apoyo para el Jefe de la Unidad, situación que no se está presentando*", es así que luego del análisis realizado en el presente seguimiento se establece que, para efectuar la implementación del Oficial de seguridad, sería necesario realizar algunos ajustes a los decretos (Decreto 4780 del 2008, Resolución 035 del 2022 y así mismo al Decreto 4781 del 2008) que establecen la planta

de personal del HOMIL, creando un nuevo cargo, lo cual requiere una modificación a la estructura organizacional, la cual no depende únicamente del Hospital Militar, debido a que se requiere de la aprobación de algunas entidades, entre ellas el Departamento Administrativo de la Función Pública y el Ministerio de Defensa. En línea con lo anterior, y considerando que la entidad ha adelantado estrategias para dar cumplimiento a la necesidad de contar con el Oficial de Seguridad de la Información, se determina no mantener lo observado en el anterior seguimiento y realizar la siguiente recomendación:

Por lo anterior, la Oficina de Control Interno, recomienda, a la Oficina Asesora de Planeación, Unidad de Talento Humano y Unidad de Informática para futura actualización de la estructura organizacional, incluir la Oficina del Oficial de Seguridad, con el propósito de dar cumplimiento a la resolución 500 de MinTIC del 10 de marzo 2021 en el numeral 6 ítem 9 y en el anexo 1 numeral 7.2.3, donde hace referencia a la determinación de los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad, recursos que deben manejarse de manera diferenciada a los de la Unidad de Informática de HOMIL, así mismo revisar y evaluar el procedimiento con el fin de efectuar ajustes en relación al rol del responsable del MSPI, de acuerdo a la normatividad vigente.

7 CONCLUSIONES

1. Se realizó seguimiento al diseño e implementación del Modelo de Seguridad y Privacidad de la Información MPSI de HOMIL, de conformidad con lo establecido en la normatividad vigente, en relación al modelo de privacidad y seguridad de los sistemas de información, manuales, protocolos, políticas, planes y procedimientos, y se verificaron los lineamientos y directrices establecidos por MinTIC.
2. Durante el seguimiento al Modelo de Seguridad y Privacidad de la Información HOMIL, por parte de la Oficina de Control Interno se pudo verificar que, desde la elaboración del Diagnóstico y del Plan de Trabajo, así como la permanente actualización y mejora de los documentos e instrumentos que se desprenden del Modelo, han sido elaborados y actualizados siguiendo las directrices del MINTIC.
3. Se verificó que se encuentra establecida la Política General de Seguridad y Privacidad de la Información y que la misma atendió las recomendaciones de la "Guía - Elaboración de la política general de seguridad y privacidad de la información", generada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC – versión 2016.

4. Se estableció que existe un documento que define los "Roles y Responsabilidades de Seguridad de la Información" GT-UNIN-PL-04", requeridos para asegurar que el MSPI de HOMIL, sea implementado, mantenido y mejorado continuamente en la entidad, no obstante, no está creada el área de seguridad Digital, sino que aparece relacionada con un rol dentro de la Unidad de Informática de HOMIL.

8. RECOMENDACIÓN

1. Se recomienda elaborar acciones encaminadas a mejorar los resultados del autodiagnóstico y contribuir con el cierre de Brechas Nivel de Madurez por dominios y controles en los temas de criptografía, seguridad de las operaciones, seguridad de las comunicaciones y adquisición, desarrollo y mantenimiento de sistemas, según lo lineamientos de la resolución 0500 del 10 de marzo de 2023; anexo 1, con la definición, documentación y socialización de las políticas y procedimientos, conforme lo establecido en la norma ISO27001:2022.

Tabla 6 Recomendaciones y Responsables

RECOMENDACIÓN	RESPONSABLE
1 y 2	Unidad Informática
3	Oficina Asesora de Planeación, Unidad de Talento Humanos y Unidad Informática

Revisó:

SANDRA CAROLINA TORRES SAEZ

Jefe de Oficina Sector Defensa
Oficina de Control Interno

Elaboró: Angela Ibeth Díaz Rey.
Auditor Ingeniería de Sistemas Especialista OPS