INFORMACIÓN GENERAL

Nombre del informe	**Seguimiento a la Implementación del Modelo de Privacidad y Seguridad a los Sistemas de Información**
Dependencia (s)	**Unidad de Informática**
Auditor:	**Sandra Milena Oliveros S.**

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 y de proponer las 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.

Se 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 de evaluación al diseño, implementación y ejecución de los controles, 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 en la normatividad vigente.

3. ALCANCE

El seguimiento a la implementación del modelo de privacidad y seguridad de los sistemas de información, así como al tratamiento de riesgos, cumplimiento de políticas y lineamientos durante la vigencia 2023.

4. CRITERIO LEGAL

- ✓ Constitución Política de Colombia. Artículos 15, 209 y 269 define el derecho a la intimidad y al buen nombre.
- ✓ Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ 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.

- ✓ Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- ✓ Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- ✓ Decreto 2609 de 2012. 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.
- ✓ Decreto 2693 de 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- ✓ Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- ✓ Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 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.
- ✓ Decreto 1083 de 2015 “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 612 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 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 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 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 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.
- ✓ 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.
- ✓ DOCUMENTO TÉCNICO EXTERNO 2019, Manual para la Implementación de la Política de Gobierno Digital Implementación de la Política de Gobierno Digital (Decreto 1008 de 2018). Versión 7, abril de 2019.
- ✓ 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.
- ✓ 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
- ✓ Plan de Seguimiento, Evaluación y Análisis del MSPI GT-SEGU-PL-01 V1
- ✓ Plan de Sensibilidad y Capacitación en Seguridad de la Información GT-UNIN-PL-06 V1
- ✓ Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2
- ✓ Documento Informativo Para la Gestión de Incidentes de Seguridad de la Información - GT-GERE-PR-01-DI-01_V1
- ✓ 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
- ✓ Política General de Seguridad y Privacidad de la Información - GT-UNIN-PO-01 V1

- ✓ Guía para la administración del riesgo y el diseño de control en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital Versión 6 del Departamento Administrativo de la Función Pública (DAFP) noviembre de 2022.

5. METODOLOGIA

La metodología se fundamentó en el levantamiento de información producto de solicitud de documentos y visita in situ efectuado en la Unidad de Informática.

Las actividades realizadas se detallan a continuación:

- Solicitud de información: Se solicitó información asociadas al MPSI (Modelo de Privacidad y Seguridad de la Información) y a su implementación en la entidad entre las que se destacan las siguientes:

INFORMACION	RECIBIDA
1. Composición personal de planta y bajo la modalidad de contrato de prestación de servicios de la Unidad de Informática.	✓
2. Protocolo de seguridad informática	✓
3. Plan de mitigación frente a la pérdida de información.	✓
4. Soporte de los controles de acuerdo al mapa de riesgos institucional correspondiente al 2 semestre de 2022.	✓
5. Contratos vigentes celebrados para auditoría de sistemas en la entidad.	✓
6. Procedimientos, manuales e instructivos diseñados para dar cumplimiento a lo establecido en la Ley 1712 de 2014 Transparencia y acceso a la información y en la Resolución 1519 de 2020.	✓
7. Reportes de información vigencia 2022 al Ministerio de Tecnologías de la Información y las Comunicaciones	✓
8. Política de seguridad y privacidad de la información	✓
9. Licencias de los aplicativos y programas que utiliza la entidad.	✓
10. Procedimiento de Backup y restauración de datos	✓
11. Protocolo cadena de custodia digital.	✓

12. Plan de tratamiento de riesgos de la seguridad de la información	✔
13. Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información	✔
14. Procedimiento y plan de tratamiento de gestión de riesgos de seguridad de la información.	✔
15. Declaración de aplicabilidad	✔
16. Plan de capacitación, sensibilización y comunicación de seguridad de la información	✔

- Entrevista presencial: Llevada a cabo el pasado 12 de julio de 2023 con el fin de aclarar incertidumbres del proceso de implementación del modelo de privacidad y seguridad de los sistemas de información (MSPI) y posteriormente el 15 de septiembre de 2023, día en el que se realizó solicitud de documentos adicionales.

Para la evaluación y verificación del proceso de seguridad de la información, se estableció en el alcance evaluar y verificar el proceso de seguridad de la información con énfasis en la fase de implementación del MSPI que se está llevando a cabo en la entidad.

6. RESULTADOS DEL SEGUIMIENTO

La Oficina de Control Interno pudo evidenciar que la Unidad de Informática, ha venido realizando ajustes y modificaciones a los procesos y procedimientos en aras a establecer, implementar, mantener y mejorar el Modelo de Seguridad y Privacidad de la Información el cual se encuentra en proceso de ejecución e implementación.

6.1 Responsable del MSPI

6.1.1 Condición:

La Unidad de Informática está conformada por 23 funcionarios de los cuales, 10 son de planta y 13 de contrato por prestación de servicios así:

Área	N° Funcionarios		
	Planta	Contrato OPS	TOTAL
Jefatura	1		1

Infraestructura y Comunicaciones - INCO	2	3	5
Gestión de Aplicaciones y Movilidad - GEAM	4	2	6
Gestión de Requerimientos e Incidentes - GERE	1	1	2
Gestión de Seguridad Informática - GESU			0
Mesa de Servicio de Tecnologías de la información - MSTI	2	7	9
TOTAL			**23**

Fuente: Información suministrada por la Unidad de Informática HOMIL

NOTA: A la fecha la Unidad de Informática tiene pendiente la contratación por prestación de servicios de un Ingeniero especialista en Seguridad de la Información o seguridad informática; el responsable de la Unidad de Informática manifiesta que no ha sido posible su vinculación aduciendo que el ingreso es muy bajo; se están incorporando dos (2) tecnólogos de sistemas o afines para apoyar estas actividades teniendo en cuenta que el Jefe de la unidad tiene el perfil de Especialista de Seguridad de la Información

6.1.2 Criterio:

PLAN	PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION 2022	CÓDIGO	GT-UNIN-PL-05	VERSIÓN	01
		Página:		11 de 19	

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

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

Fuente: Plan de Seguridad y Privacidad de la Información 2022 Fecha de actualización: 17/01/2022

6.1.3 Causa:

Posible falta de personal con el perfil especializado y conocimiento que se requiere para el manejo de una implementación de un Modelo de Privacidad y Seguridad de la Información para la entidad.

6.1.4 Consecuencia:

Posible incumplimiento al numeral 8.2.2 del plan de privacidad y seguridad de la información GT-UNIN-PL-05 V1 establecido y diseñado por el HOMIL.

6.1.5 Hallazgo 1:

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.

6.1.6 Recomendaciones:

Se recomienda evaluar la opción de nombramiento formal a través de acto administrativo a una persona de planta en carrera administrativa como Oficial de Seguridad de la Información, tal como se encuentra establecido en el plan de seguridad y privacidad de la información 2022 con fecha de actualización 17/01/2022.

La OCIN recomienda 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.

6.2 Protocolo de Seguridad Informática

6.2.1 Condición

La entidad cuenta con el manual de políticas de seguridad y privacidad de la información GT-UNIN-MN-03 V2, el cual fue adoptado por el HOMIL a través de la Directiva Permanente No. 002 del 15 de junio de 2021; el cual contiene una serie de lineamientos dirigidos a todos los responsables de la seguridad y privacidad de la información propuesto y definido por la entidad.

6.2.2 Criterio

ÍNDICE

1. JUSTIFICACION.

Con este documento se establecen los lineamientos de seguridad y privacidad de la información para el correcto uso de los activos informáticos puestos a disposición del personal que labora en el Hospital Militar Central, las cuales deben ser aplicadas durante el cumplimiento de sus objetivos. Dichos lineamientos estarán enfocados a mitigar los riesgos de Integridad, Disponibilidad y Confidencialidad de los activos informáticos.

Fuente: Manual de Políticas de Seguridad y Privacidad de la Información V2 HOMIL

6.2.3 Recomendación

La OCIN recomienda continuar con la actualización permanente del manual con el fin de estar articulado a los nuevos lineamientos que estipule el MinTIC y el MINDEFENSA en materia de privacidad y seguridad de la información.

6.3 Plan de mitigación frente a la pérdida de información y plan de continuidad del negocio

6.3.1 Condición

Se evidencia la existencia del procedimiento GT-UNIN-PR-05 V1 Continuidad de servicios de salud ante una interrupción en la prestación de servicios tecnológicos y su aplicabilidad junto con el reporte de gestión de incidentes de seguridad informática.

6.3.2 Criterio

HOSPITAL MILITAR CENTRAL	PROCEDIMIENTO: CONTINUIDAD DE SERVICIOS DE SALUD ANTE UNA INTERRUPCIÓN EN LA PRESTACIÓN DE SERVICIOS TECNOLÓGICOS	CÓDIGO: GT-UNIN-PR-05
	UNIDAD: INFORMÁTICA	FECHA DE EMISIÓN: 18-03-2022
		VERSIÓN: 01
	PROCESO: TECNOLOGIAS DE LA INFORMACIÓN	Página 1 de 10
	SISTEMA DE GESTION INTEGRADO SGI	

1. OBJETIVO

Establecer y coordinar las acciones pertinentes para garantizar la continuidad de la operación y la prestación de servicios de salud en el Hospital Militar Central – HOMIL, mediante la activación de un plan de contingencia en caso de una interrupción causada por un evento natural o provocado por el hombre de uno de los servicios tecnológicos identificado como crítico.

2. ALCANCE

Es aplicable a todos los servicios asistenciales del Hospital Militar Central desde el reporte de la interrupción de alguno de los servicios tecnológicos clasificado como crítico en el Análisis de Impacto de Negocio – BIA (GT-UNIN-MN-02-DI-03) hasta el restablecimiento del servicio informático afectado.

3. DEFINICIONES PROPIAS DEL PROCEDIMIENTO

Gestión de continuidad de negocio (BCM): Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

Plan de Continuidad de Negocio: Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción.
Nivel de Criticidad: Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Interrupción: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Resiliencia: Habilidad Capacidad para que una organización para resistir cuando es afectada al ser afectada por una interrupción.

Disparador o detonante: Evento que hace que el sistema inicie una respuesta.

Fuente: Procedimiento Continuidad de Servicios de Salud ante una Interrupción en la Prestación de Servicios Tecnológicos

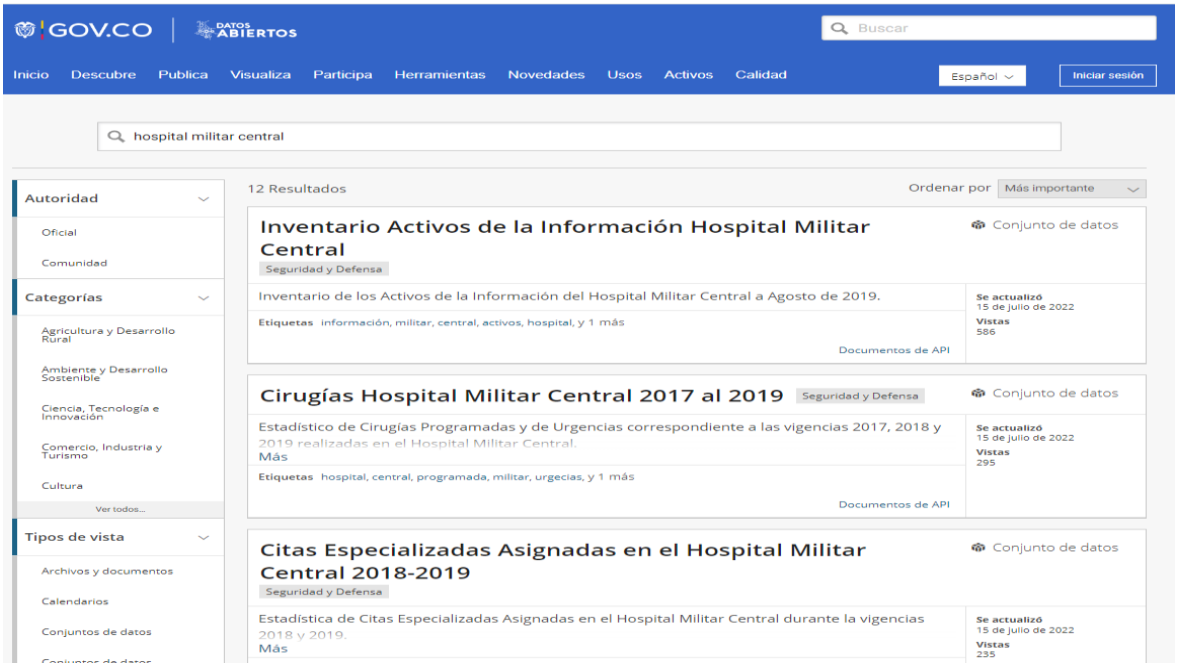
6.3.3 Recomendación

Continuar con la gestión de casos y eventos reportados con el fin de mitigar los riesgos por pérdida de información o interrupción en la prestación de servicios de salud.

6.4 Procedimientos, manuales e instructivos diseñados para dar cumplimiento a lo establecido en la Ley 1712 de 2014 Transparencia y acceso a la información y a la Resolución 1519 de 2020.

6.4.1 Condición

Se evidencia directrices implementadas en la página web de la entidad referente a los requisitos en materia de accesibilidad web, seguridad digital y datos abiertos como se puede apreciar a continuación:


GOV.CO
DATOS ABIERTOS
Buscar
Inicio Descubre Publica Visualiza Participa Herramientas Novedades Usos Activos Calidad
Español
Iniciar sesión
hospital militar central
Autoridad
Oficial
Comunidad
Categorías
Agricultura y Desarrollo Rural
Ambiente y Desarrollo Sostenible
Ciencia, Tecnología e Innovación
Comercio, Industria y Turismo
Cultura
Ver todos...
Tipos de vista
Archivos y documentos
Calendarios
Conjuntos de datos
12 Resultados
Ordenar por
Más importante
Inventario Activos de la Información Hospital Militar Central
Conjunto de datos
Seguridad y Defensa
Inventario de los Activos de la Información del Hospital Militar Central a Agosto de 2019.
Etiquetas información, militar, central, activos, hospital, y 1 más
Documentos de API
Se actualizó 15 de julio de 2022
Vistas 586
Cirugías Hospital Militar Central 2017 al 2019
Seguridad y Defensa
Conjunto de datos
Estadístico de Cirugías Programadas y de Urgencias correspondiente a las vigencias 2017, 2018 y 2019 realizadas en el Hospital Militar Central.
Más
Etiquetas hospital, central, programada, militar, urgecias, y 1 más
Documentos de API
Se actualizó 15 de julio de 2022
Vistas 295
Citas Especializadas Asignadas en el Hospital Militar Central 2018-2019
Conjunto de datos
Seguridad y Defensa
Estadística de Citas Especializadas Asignadas en el Hospital Militar Central durante la vigencias 2018 y 2019.
Más
Se actualizó 15 de julio de 2022
Vistas 235


GOV.CO
COLOMBIA POTENCIA DE LA VIDA
Registro Mi portal Iniciar Sesión Mapa
Buscar en sede electrónica
HOSPITAL MILITAR CENTRAL
Inicio La Institución Transparencia Institucional Atención y Servicios a la Ciudadanía Participa Educación Normatividad Comunicaciones
1. Información de la Entidad
2. Normatividad
3. Contratación
4. Planeación, Presupuesto e Informes
5. Trámites y Servicios
6. Participa
7. Datos abiertos
8. Información específica para Grupos de Interés
9. Obligación de reporte de información
Inicio > Transparencia Institucional > 7. Datos abiertos
7. Datos abiertos
7.1 Instrumentos de gestión de la información
7.1.1 Registros de activos de información
7.1.2 Índice de información clasificada y reservada
7.1.3 Esquema de publicación de la información
7.1.4 Programa de gestión documental
7.1.5 Tablas de retención documental
7.1.6 Costos de reproducción de información pública
7.1.7 Cuadros de Clasificación Documental
7.1.8 Registro de Publicaciones
7.2 Sección de Datos Abiertos

Fuente: Página web HOMIL

6.4.2 Criterio

RESOLUCIÓN 1519 DE 2020
(agosto 24)

por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

RESUELVE:

Artículo 1°. *Objeto.* La presente resolución tiene por objeto expedir los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD).

Artículo 2°. Ámbito de aplicación y sujetos obligados. La presente resolución aplica para los sujetos obligados a que hace referencia el artículo 5° de la Ley 1712 del 2014, corregido por el artículo 1 del Decreto 1494 del 2015.

Artículo 3°. *Directrices de accesibilidad web.* A partir del 1° de enero del 2022, los sujetos obligados deberán dar cumplimiento a los estándares AA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibility Guidelines - WCAG) en la versión 2.1, expedida por el World Web Consortium (W3C), conforme con el Anexo 1 de la presente resolución aplicable en todos los procesos de actualización, estructuración, reestructuración, diseño, rediseño de sus portales web y sedes electrónicas, así como de los contenidos existentes en esas.

Artículo 4°. *Estándares de publicación y divulgación de contenidos e información.* Los sujetos obligados deberán dar cumplimiento a los estándares de publicación y divulgación de contenidos e información aplicable a sus sitios web y sede electrónica, establecidos en el Anexo 2 de la presente resolución.
Parágrafo. En cumplimiento del numeral 5 del artículo 2.1.1.3.1.1 del Decreto 1081 del 2015 los sujetos obligados deberán desarrollar el formulario electrónico para PQRSD, requisitos generales y campos mínimos que se señalen en el Anexo 2 de la presente resolución.

Artículo 5°. *Información digital archivada.* Los sujetos obligados deben garantizar y facilitar a los solicitantes, de la manera más sencilla posible, el acceso a toda la información previamente divulgada, de conformidad con el Decreto 1862 del 2015 y el artículo 16 del Decreto 2106 del 2019 o el que los modifique, subrogue o adicione. En atención a lo anterior, los sujetos obligados deben garantizar condiciones de conservación y/o archivo para posterior consulta, de la documentación digital disponible en sitios web, conforme con las Tablas de Retención Documental aprobadas acorde con los lineamientos del Archivo General de la Nación.
Los sujetos obligados no podrán eliminar información publicada en sus sitios web y deberán asegurar la preservación de documentos en ambientes electrónicos, para lo cual, deberán adoptar medidas de conservación preventiva para facilitar procesos de migración, emulación o refreshing, o cualquier otra técnica que se disponga a futuro. Para el efecto, deberán adoptar un programa de gestión documental que contemple todos los soportes de información, conforme lo dispone el Decreto 1080 del 2015, o el que lo modifique, adicione o subrogue.

Artículo 6°. Condiciones mínimas técnicas y de seguridad digital. Los sujetos obligados deberán observar las condiciones mínimas técnicas y de seguridad digital que se definen en el Anexo 3 de la presente resolución.

Artículo 7°. *Condiciones mínimas de publicación de datos abiertos.* Los sujetos obligados deberán publicar sus datos abiertos y federarlos al Portal Datos Abiertos del Estado colombiano -datos.gov.co-conforme con las directrices referidas en el Anexo 4 de la presente resolución.

Fuente: Resolución 1519 de 2020 Ministerio de Tecnologías de la Información y las Comunicaciones

6.4.3 Recomendación

Mantener las actividades que dan lugar a este cumplimiento, estableciendo controles de revisión periódica, adicionales o sin limitarse a los seguimientos efectuados por la OCIN y continuar con el cumplimiento a las disposiciones de la normatividad vigente en completitud y oportunidad.

6.5 Políticas asociadas a la Privacidad y Seguridad de la Información

6.5.1 Condición

Durante el seguimiento al Modelo de Privacidad y Seguridad de la Información la OCIN pudo evidenciar que el HOMIL cuenta con una Política General de Seguridad de la Información GT-UNIN-PO-01 V1 dando cumplimiento con los requisitos propuestos por el MSPI y la ISO 27001:2013.

Así mismo, durante la ejecución de la actividad el evidenció el documento denominado “Manual de Lineamientos de Seguridad y Privacidad de la Información” donde se relacionan las siguientes políticas y/o lineamientos aprobadas por la entidad:

POLÍTICA	UBICACIÓN DENTRO DEL MANUAL
Organización Interna	Pág. 3
Computación Móvil	Pág. 4
Teletrabajo	Pág. 5
Seguridad de los Recursos Humanos	Pág. 5
Concientización y capacitación en la seguridad de la información	Pág. 6
Gestión de activos de información	Pág. 7
Uso aceptable de los activos de información	Pág. 7
Uso de internet	Pág. 8
Uso del correo electrónico	Pág. 9
Devolución de activos	Pág. 11
Gestión de medios	Pág. 11
Control de acceso	Pág. 12
Restricción de acceso a la información	Pág. 13
Sistema de gestión de contraseñas	Pág. 13
Controles criptográficos	Pág. 14
Seguridad física y del entorno	Pág. 14
Control de acceso físico	Pág. 15
Trabajo en áreas seguras	Pág. 16
Seguridad de los activos informáticos -	Pág. 17
Seguridad y mantenimiento de los equipos	Pág. 18
Retiro de activos	Pág. 19
Seguridad de los equipos fuera de las instalaciones	Pág. 19

Fuente: Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2 HOMIL

6.5.2 Criterio

- Guía No. 2 Elaboración de la Política General de Seguridad y Privacidad de la Información – MINTIC
- ISO 27001:2013
- Resolución 7870 de 2022 MINDEFENSA

RESOLUCIÓN 7870 DE 2022

(diciembre 26)

Diario Oficial No. 52.259 de 26 de diciembre de 2022

MINISTERIO DE DEFENSA NACIONAL

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 adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.

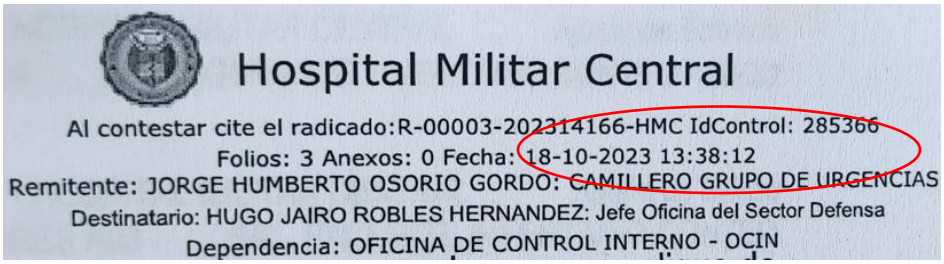
6.5.3 Recomendación

La Oficina de Control Interno recomienda a la Unidad de Informática continuar con la actualización del manual frente a los nuevos lineamientos contemplados en resoluciones aprobadas por los organismos de control en materia de Privacidad y Seguridad de la Información.

6.6 Posible vulnerabilidad a los Sistemas de Información

6.6.1 Condición:

Conforme a la queja allegada a la OCIN el pasado 18 de octubre de 2023 bajo el ID 285366, se procedió a revisar los documentos referenciados en dicho documento, realizando consulta directamente en el Sistema de Información Dinámica Gerencial donde se identificaron los siguientes, los cuales corresponden a ajustes y/o compensaciones de inventarios, registrados el 13 de octubre de 2023 para la entrega de la Farmacia de Procedimientos Menores al nuevo responsable, ingresado con el usuario de un camillero del grupo de urgencias, en el horario de 7:32 am a las 8:44 am como lo evidencia la siguiente imagen de movimiento de entrada de inventario:



Fecha Actual: 20/10/2023 5:56:12 p. m.

HOSPITAL MILITAR CENTRAL Página 1/4
830040256-0 Usuario: 53067890
Dirección: TRANSVERSAL 3A No. 49-00
Telefono: 3486868 **Movimiento de Entrada al Inventario No. EXD00000000109**
BOGOTA D.C.

Almacen: FPM - FARMACIA PROCEDIMIENTOS MENORES **Fecha:** 13/10/2023 7:32:34 a. m.
Detalle: Se realiza movimiento de inventario de entrada por compensacion de inventarios con base al id 284726 por toma fisica de inventario y entrega a nuevo responsable de farmacia Otoniel Santana Portillo **Estado:** Confirmado
Concepto: A06 - ENT. COMPENSACION INVENTARIOS
Tercero: 830040256 - HOSPITAL MILITAR CENTRAL
Dependencia:
Usuario Creacion: 1007342140 - OSORIO GORDO JORGE HUMBERTO tableCell38

Codigo	Nombre del Producto	Concen.	Unidad	Fec. Ven.	No. Lote	Cantidad	Vl Unidad	Costo Total
1032610011-QBI	AGUA DESTILADA 500ml BOLSA 500mL L-230634853 - 30/06/2026	500mL	99 - BOLSA	30/06/2026	230634853	3,00	$2.480,00	$7.440,00
E1032610011-QBI	AGUA DESTILADA X 500mL BOLSA 500mL L-221122442 - 30/11/2025	500mL	99 - BOLSA	30/11/2025	221122442	47,00	$2.480,00	$116.560,00
1199010022	AGUJA CHIBA De 18 g a 22 g X 9cm O 10cm a 20 cm. UNIDAD 18X15 CMS L-011368967 - 01/06/2026	18X15 CMS	7 - UNIDAD	1/06/2026	011368967	3,00	$55.175,40	$165.526,20
1176090789	AGUJA MONOPOLAR PARA INYECCION DE TOXINA BUTILINICA UNIDAD 37mm L-055038 - 01/09/2025	37mm	7 - UNIDAD	1/09/2025	055038	1,00	$121.721,85	$121.721,85

A continuación relaciono los documentos registrados con el usuario referenciado en la parte superior en el Sistema Dinámica Gerencial, incluyendo los valores correspondientes a los movimientos de inventarios:

DOCUMENTO DINÁMICA GERENCIAL	CONCEPTO	VALOR
EXD00000000109	MOVIMIENTO DE ENTRADA AL INVENTARIO	$3.580.266,57
EXD00000000110	MOVIMIENTO DE ENTRADA AL INVENTARIO	$1.353.734,24
SXD00000000021	MOVIMIENTO DE SALIDA AL INVENTARIO	$3.580.266,57
SXD00000000022	MOVIMIENTO DE SALIDA AL INVENTARIO	$146.496,18

6.6.2 Criterios:

- Numeral 6.12. Sistema de Gestión de Contraseñas – ISO/IEC 27001:2013

6.12. SISTEMA DE GESTIÓN DE CONTRASEÑAS – Ref.: ISO/IEC 27001:2013 CL. A.9.4.3

a. La administración, así como la entrega de las contraseñas a los usuarios debe seguir el procedimiento Gestión de Usuarios y contraseñas.

b. Los usuarios deben seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

1. Las contraseñas son de uso personal y por ningún motivo se deben prestar a otros usuarios.
2. Las contraseñas no deben ser reveladas.
3. Las contraseñas no se deben escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento Gestión de Usuarios y Contraseñas.

SI ENCUENTRA ESTE DOCUMENTO IMPRESO, TENGA EN CUENTA QUE ES UNA COPIA NO CONTROLADA; POR FAVOR REMITIRSE A LA INTRANET INSTITUCIONAL
FT-CLDD-01_V4

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.

Fuente: Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2

- Manual Operativo del Modelo Integrado de Planeación y Gestión CONSEJO PARA LA GESTIÓN Y DESEMPEÑO INSTITUCIONAL Versión 5 en el numeral *"3.4.2. Política de Seguridad Digital En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades".*

  Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

- Procedimiento: Creación de usuarios y asignación de Permisos GT-UNIN-PR-04 V2 cuyo objetivo y alcance definido por la entidad es el siguiente:

  "OBJETIVO Establecer las directrices y lineamientos para la creación de credenciales de acceso a los sistemas de Información y las tecnologías de la información que los soportan, teniendo en cuenta la asignación de permisos según su rol o perfil requerido para desempeñar sus funciones dentro del Hospital Militar Central"

  "ALCANCE: Comprende desde la solicitud de acceso a los sistemas de información y la infraestructura que los soportan hasta el procedimiento de baja de las credenciales; incluyendo la creación del usuario, asignación de perfil y rol para el personal de planta, contratistas, terceros, talento humano en salud en formación, militares en comisión y entes reguladores"

6.6.3 Causa:

Posiblemente desconocimiento de los lineamientos definidos en el Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2 en materia del Sistema de Gestión de Contraseñas y el procedimiento: "Creación de usuarios y asignación de permisos" GT-UNIN-PR-04 V2 diseñados y aprobados por la entidad.

6.6.4 Consecuencia:

Pérdida de la confidencialidad por mal manejo de las credenciales de acceso al sistema de información

6.6.5 Hallazgo 2:

La OCIN evidenció incumplimiento al numeral 6.2. Sistema de Gestión de contraseñas de acuerdo a lo definitivo en el Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 y al procedimiento "Creación de usuarios y asignación de Permisos GT-UNIN-PR-04 V2".

6.6.6 Recomendación:

La OCIN recomienda fortalecer la campaña de sensibilización para el conocimiento y aplicación de los lineamientos y directrices contemplados en el Manual de Lineamientos de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2 y el procedimiento, Creación de usuarios y asignación de Permisos GT-UNIN-PR-04 V2

6.7 Licencias de los aplicativos y programas que utiliza la entidad.

6.7.1 Condición

NO.	SOFTWARE	CANTIDAD	CANTIDAD DISPONIBLE	NO.	SOFTWARE	CANTIDAD	CANTIDAD DISPONIBLE	NO.	SOFTWARE	CANTIDAD	CANTIDAD DISPONIBLE
1	Google Workspace Enterprise Plus	300	278	28	Ciesa	No Aplica	No Aplica	55	DUSOFT	No Aplica	No Aplica
2	Google Workspace Enterprise Starter	1000	34	29	Cisne	No Aplica	No Aplica	56	SIGEP	No Aplica	No Aplica
3	Google Workspace Frontline Starter	1500	95	30	Yubi	No Aplica	No Aplica	57	CETIL	No Aplica	No Aplica
4	Chrome Enterprise	400	400	31	BTR – Bitácora de residentes	No Aplica	No Aplica	58	Servicio Contac Center	No Aplica	No Aplica
5	Adobe Acrobat	ILIMITADAS	ILIMITADAS	32	Aula Virtual	No Aplica	No Aplica	59	SERVICIO DE IMPRESION PAPER CUT	No Aplica	No Aplica
6	Office 2013 profesional	278	0	33	REPNEUROVIZ-EDU	No Aplica	No Aplica	60	DIGITURNO CONSULTA EXTERNA	14	14
7	Office 2016	47	10	34	Suite VE	No Aplica	No Aplica	61	DIGITURNO URGENCIAS	Ilimitadas	Ilimitadas
8	Anthro-Antho Plus	ILIMITADAS	ILIMITADAS	35	Saberes	No Aplica	No Aplica	62	DIGITURNO ATENCION AL USUARIO	1	1
9	Net Framework	ILIMITADAS	ILIMITADAS	36	Intranet institucional	WEB	WEB	63	Servicio de conectividad WiFi	WEB	WEB
10	DameWare	11	0	37	Página Web Corporativa	WEB	WEB	64	Servicio de Backup Veeam Backup,	X	X
11	Teams	ILIMITADAS	ILIMITADAS	38	Unilog	No Aplica	No Aplica	65	CONTROL DE ACCESO	No Aplica	No Aplica
12	7 Zip	ILIMITADAS	ILIMITADAS	39	MOSAIQ - Radioterapia	No Aplica	No Aplica	66	VMWARE	No Aplica	No Aplica
13	Toad	1	1	40	Pediatrix	No Aplica	No Aplica	67	SIPOST	ILIMITADA	ILIMITADA
14	VPN	ILIMITADAS	ILIMITADAS	41	QSYS	ILIMITADAS	ILIMITADAS	68	CARTELERA DIGITAL	12	12
15	Creative Cloud Desktop Application(5.10.0)	4	4	42	SARLAFT	WEB	WEB	69	MESA DE SERVICIO	21	21
16	Autocad - autocad architecture - autocad electricalun - autocad mep - autocad map 3d - autocad mechanicalcreado - autocad plant 3dthis - autocad raster designraster autocad web - autocad web - mobile app autocad for macautocad,	1	0	43	Sistema de información Gestor Documental – Control Doc	WEB	WEB	70	LANSWEEPER	WEB	WEB
17	Dinamica Gerencial	ILIMITADAS	ILIMITADAS	44	RUAF	WEB	WEB	71	AIRE ACONDICIONADO	2	0
18	Dinamica web	ILIMITADAS	ILIMITADAS	45	SALUD.SIS	WEB	WEB	72	ALTAI WIFI	WEB	WEB
19	Dinamica fox	ILIMITADAS	ILIMITADAS	46	SIIF NACION	WEB	WEB	73	SERVIDORES APAGADO	WEB	WEB
20	Visual Medical (RIS)	web	web	47	SECOP	WEB	WEB	74	GENESISI CALL CENTER	WEB	WEB
21	Enterprise (LIS)	WEB	WEB	48	SIVIGILA	ILIMITADA	ILIMITADA	75	cisco telefonia	400 telefonos ext 9000	400 telefonos ext 9000
22	Hexaban	WEB	WEB	49	OLIMPIA	WEB	WEB	76	Chomeos	Ilimitadas	Ilimitadas
23	HistHOMIL	APLICACION	APLICACION	50	SIRECI	WEB	WEB	77	MICRODICOM	Ilimitadas	Ilimitadas
24	Sistema de gestión de Calidad	No Aplica	No Aplica	51	ADRES	WEB	WEB	78	FORTINET	No Aplica	No Aplica
25	THAIS	No Aplica	No Aplica	52	PISIS			79	SOLARWIN	No Aplica	No Aplica
26	Promed	No Aplica	No Aplica	53	CHIP	Ilimitadas	Ilimitadas	80	Epiclatino	WEB	WEB
27	Kayros	No Aplica	No Aplica	54	3M	No Aplica	No Aplica				

Fuente: Información Suministrada por la Unidad de Informática

6.7.2 Criterio

PLAN	PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION 2022	CÓDIGO	GT-UNIN-PL-05	VERSIÓN	01
		Página:		13 de 19	

8.3. ROLES, RESPONSABILIDADES Y AUTORIDADES

8.3.1. Director General

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

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

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

Fuente: Plan de Privacidad y Seguridad de la Información 2022

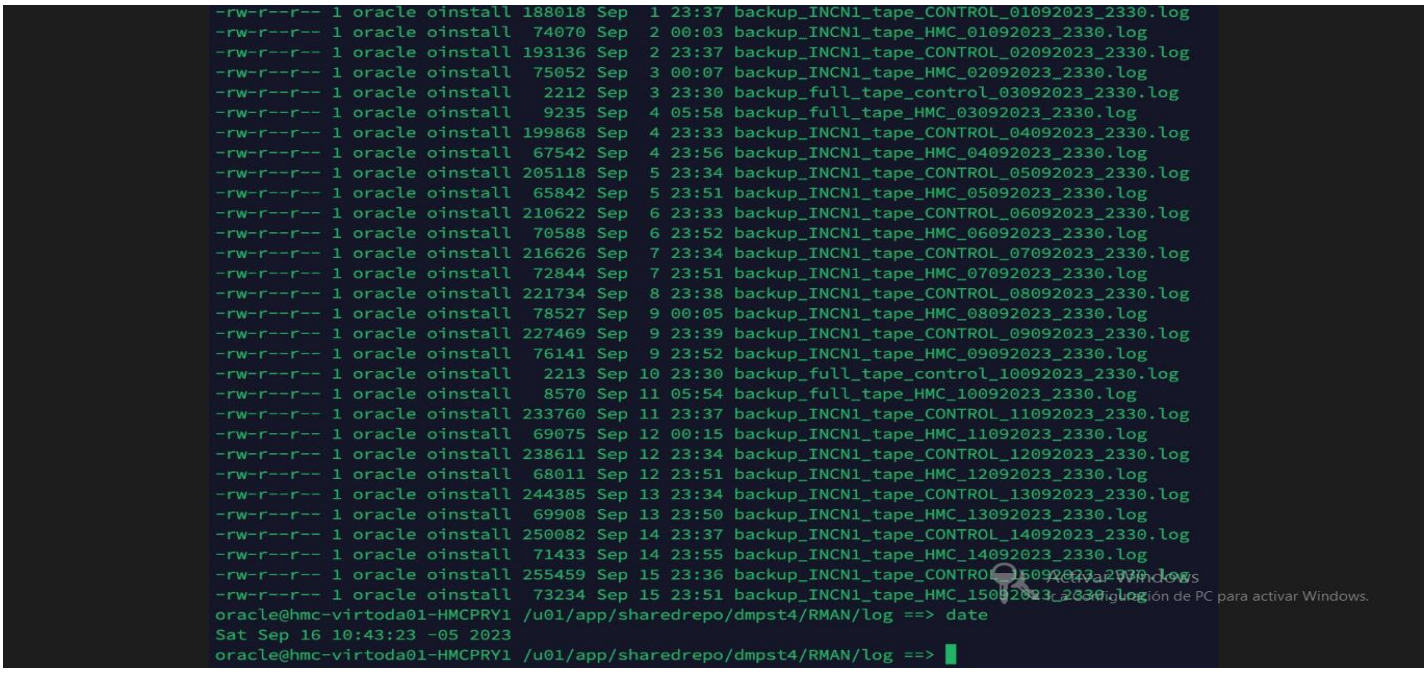
6.7.3 Recomendación

Continuar con el control y velar por que todo el sistema de información adquirido o desarrollado estén debidamente soportados y con licencias actualizadas según el caso.

6.8. Procedimiento de Backup y restauración de datos

6.8.1 Condición

Se evidencia la realización periódica de copias de respaldo del Sistema de Información Dinámica Gerencial Hospitalaria, ControlDoc, Suite vision y cuentas de office 365 con acceso a OneDrive de los funcionarios del HOMIL pertenecientes al grupo de la Escuela de Auxiliares de Enfermería de acuerdo con el Protocolo: Gestión de Copias de Respaldo y Recuperación en Escuela de Auxiliares – GT-GESU-PT-01.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
hmcdg-scan Oracle backup (Respositorio SAN Hitachi)	Oracle RMAN Backup	1	Stopped	5 days ago	Failed	<Not scheduled>	Respositorio SAN Hitachi
SEGURIDAD RED	VMware Backup	3	Stopped	9 hours ago	Failed	16/09/2023 23:00	Repositorio SAN Hitachi 2
VARIOS	VMware Backup	5	Stopped	9 hours ago	Failed	16/09/2023 22:45	Repositorio SAN Hitachi 2
AD	VMware Backup	5	Stopped	10 hours ago	Warning	16/09/2023 22:45	Repositorio SAN Hitachi 2
AMAREY	VMware Backup	7	Stopped	9 hours ago	Warning	16/09/2023 23:45	Repositorio SAN Hitachi 2
CALL CENTER	VMware Backup	3	Stopped	9 hours ago	Warning	16/09/2023 23:45	Repositorio SAN Hitachi 2
CIEL	VMware Backup	3	Stopped	11 hours ago	Warning	16/09/2023 21:15	Repositorio SAN Hitachi 2
CONTROL ACCESO CCTV	VMware Backup	3	Stopped	9 hours ago	Warning	16/09/2023 23:30	Repositorio SAN Hitachi 2
DG_WEB	VMware Backup	7	Stopped	11 hours ago	Warning	16/09/2023 22:00	Repositorio SAN Hitachi 2
DINAMICA - TAB CONTROL	VMware Backup	3	Stopped	10 hours ago	Warning	16/09/2023 23:00	Repositorio SAN Hitachi 2
DROSERVICIO	VMware Backup	4	Stopped	10 hours ago	Warning	16/09/2023 23:00	Repositorio SAN Hitachi 2
FILESERVER	VMware Backup	3	Stopped	11 hours ago	Warning	16/09/2023 22:00	Repositorio SAN Hitachi 2
GESTION DOCUMENTAL	VMware Backup	3	Stopped	10 hours ago	Warning	16/09/2023 22:15	Repositorio SAN Hitachi 2
HMC 1	VMware Backup	2	Stopped	12 hours ago	Warning	16/09/2023 21:00	Repositorio SAN Hitachi 2
HMC 2	VMware Backup	5	Stopped	9 hours ago	Warning	16/09/2023 23:15	Repositorio SAN Hitachi 2
hmcdg-scan Oracle backup (Repositorio SAN Hitachi 2)	Oracle RMAN Backup	1	Stopped	9 hours ago	Warning	<Not scheduled>	Repositorio SAN Hitachi 2
IMPRESION	VMware Backup	1	Stopped	11 hours ago	Warning	16/09/2023 22:00	Repositorio SAN Hitachi 2
INTRANET - MICROSITIOS	VMware Backup	2	Stopped	10 hours ago	Warning	16/09/2023 22:15	Repositorio SAN Hitachi 2
LABORATORIO	VMware Backup	4	Stopped	10 hours ago	Warning	16/09/2023 22:30	Repositorio SAN Hitachi 2
MESA DE SERVICIO	VMware Backup	2	Stopped	11 hours ago	Warning	16/09/2023 21:30	Repositorio SAN Hitachi 2
OPS	VMware Backup	2	Stopped	10 hours ago	Warning	16/09/2023 23:00	Repositorio SAN Hitachi 2
ORION	VMware Backup	4	Stopped	9 hours ago	Warning	16/09/2023 23:30	Repositorio SAN Hitachi 2
SUITE SARLAFT	VMware Backup	3	Stopped	11 hours ago	Warning	16/09/2023 21:45	Repositorio SAN Hitachi 2
THAIS - DESARROLLO UNTH	VMware Backup	3	Stopped	10 hours ago	Warning	16/09/2023 22:30	Repositorio SAN Hitachi 2
VEEAM BACKUP	VMware Backup	4	Stopped	10 hours ago	Warning	After [IMPRESION]	Repositorio SAN Hitachi 2

Fuente: Información suministrada por la Unidad de Informática

6.8.2 Criterio

MANUAL	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CODIGO	GT-UNIN-MN-03	VERSION	01
		Página:		24 de 38	

6. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

b. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código móvil y malicioso.

c. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Unidad de Informática y deberán ser actualizados permanentemente.

d. No está permitido descargar software o archivos de fuentes externas a los recursos institucionales a través de Internet u otra red pública.

e. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

f. Todos los medios de almacenamiento que se conecten a equipos del Hospital Militar Central deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

g. El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por el Oficial de Seguridad de la Información (o quien hagan sus veces).

h. El Hospital Militar Central será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

i. Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

6.17. COPIAS DE RESPALDO – Ref.: ISO/IEC 27001:2013 CL. A.12.3

a. Se debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Unidad de Informática y las dependencias responsables de la misma, contenida en la plataforma tecnológica del Hospital Militar Central, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente

Fuente: Manual de Políticas de Seguridad y Privacidad de la Información - HOMIL

6.8.3 Recomendación

Continuar con las copias de seguridad, respaldo y resguardo a los sistemas de información con los que cuenta la entidad, con el fin de mitigar el riesgo de pérdida de información frente a una catástrofe informática, natural o ataque cibernético.

6.9 Declaración de aplicabilidad

6.9.1 Condición

El HOMIL cuenta con la Declaración de Aplicabilidad en materia de seguridad de la información, conforme a los controles de la norma ISO 27001 2013 y se mantiene actualizada durante su fase de implementación:

HOSPITAL MILITAR CENTRAL	ANEXO: DECLARACIÓN DE APLICABILIDAD	CÓDIGO: GT-UNIN-MN-03-FT-01
	UNIDAD: INFORMÁTICA	FECHA DE EMISIÓN: 24-08-2022
		VERSIÓN: 01
	PROCESO: TECNOLOGÍAS DE LA INFORMACIÓN	Página 1 de 1
	SISTEMA DE GESTION INTEGRADO SGI	

Núme	Nombre	Implementado / Exclusi	Aplicado Actualmen (Si /No)	Justificación de Exclusió	Control que se aplicó	Responsable de Ejecutar el control	Observaciones / Evidencias
A.5	Políticas de seguridad de la información						
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	Lineamiento: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.					
A.5.1.1	Políticas para la seguridad de la información	Implementado	Si		* Directiva Permanente Política de Seguridad de la información	Unidad de Informática - GESU	* Pendiente la aprobación de la Directiva Permanente - Política de Seguridad de la Información * No se encuentra el documento actual vigente de la política de seguridad de la información en la intranet ni en la pagina web

Fuente: Anexo Declaración de Aplicabilidad HOMIL

6.9.2 Criterio

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

2. REFERENCIA NORMATIVA

El siguiente documento referenciado es indispensable para la aplicación de esta norma. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento referenciado (incluida cualquier corrección).

NTC-ISO/IEC 17799:2006, Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de esta norma, se aplican los siguientes términos y definiciones:

3.1
aceptación del riesgo
decisión de asumir un riesgo.

[Guía ISO/IEC 73:2002]

3.2
activo
cualquier cosa que tiene valor para la organización.

[NTC 5411-1:2006]

3.3
análisis de riesgo
uso sistemático de la información para identificar las fuentes y estimar el riesgo.

[Guía ISO/IEC 73:2002]

3.4
confidencialidad
propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[NTC 5411-1:2006]

3.5
declaración de aplicabilidad

documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

NOTA Los objetivos de control y los controles se basan en los resultados y conclusiones de los procesos de valoración y tratamiento de riesgos, requisitos legales o reglamentarios, obligaciones contractuales y los requisitos del negocio de la organización en cuanto a la seguridad de la información.

Fuente: ISO 27001:2013

6.9.3 Recomendación

- Llevar control de los riesgos de seguridad digital consolidado con el fin de establecer un seguimiento a los planes de mejora, registro de materialización de riesgos y que pueda alimentar la matriz de riesgos institucional catalogados con tipología de corrupción y de gestión.

6.10 Plan de capacitación, sensibilización y comunicación de seguridad de la información

6.10.1 Condición

Se evidencian campañas de sensibilización en seguridad de la información de manera periódica como se puede observar a continuación:

Fuente: Información suministrada por la Unidad de Informática

6.10.2 Criterio

PLAN	PLAN DE SENSIBILIZACIÓN y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GT-UNIN-PL-06	VERSIÓN	01
		Página:		8 de 12	

5.4.1. Socializar a los funcionarios de planta y de contrato de los procesos estratégicos, misionales, de apoyo y de evaluación que reciben, crean, procesan, gestionan, administran transmiten o resguardan información del Hospital Militar Central las buenas practicas relacionadas con la seguridad de la información con el fin de que sean aplicadas en sus labores diarias y así minimizar los eventos de seguridad reportados a la mesa de servicio.

5.4.2. Fomentar la cultura de seguridad digital en los funcionarios para que sea implementada en sus labores cotidianas y así tratar de mitigar los riesgos.

5.4.3. Socializar a los funcionarios los principales riesgos de seguridad de la información.

5.4.4. Indicador: Ejecución Plan de sensibilización de la Seguridad y la Privacidad de la Información.
Formula: (No. de actividades programadas / No. de actividades ejecutadas) * 100
Meta: 85%
Periodicidad: Semestral

5.4.5. Indicador: Establecer la efectividad del plan de sensibilización de la Seguridad y la Privacidad de la Información.
Formula: (No. de fallas encontradas en las sensibilizaciones / No. total de personal a capacitar) * 100
Meta: 80% - 90%
Periodicidad: Semestral

6. DESARROLLO DEL PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

6.1. Técnicas que se usarán en el programa de sensibilización y capacitación en seguridad de la información

Las técnicas que se utilizarán en el programa de sensibilización en seguridad de la información son las relacionadas a continuación:

1. Tips de Seguridad de la información, los cuales serán enviados cada 15 días vía correo electrónico a los funcionarios del Hospital Militar Central.
2. Charlas con temas relacionados en de Seguridad de la información vía Teams
3. Eventos relacionados con seguridad
4. E-learning (presentaciones con información sobre seguridad de la información) alojadas en la intranet o con el apoyo de una institución especializada en temas de seguridad de la información.
5. Pantallas de Bloqueo en los equipos de cómputo

Fuente: Plan de Sensibilización y Capacitación en Seguridad de la Información - HOMIL

6.10.3 Recomendación

La OCIN recomienda continuar con estas campañas de sensibilización en seguridad de la información de manera periódica a todo el personal de la entidad, con el fin conseguir que el usuario sea receptivo a éste tema, conocer los riesgos a los que se encuentran expuestos los sistemas de información, las redes, los usuarios y generar la cultura de buenas prácticas en materia de seguridad y privacidad de la información.

6.11 Gestión de incidentes de seguridad digital

La entidad define las actividades de incidentes en los siguientes documentos: Gestión de Incidentes y Requerimientos PT-GERE-PR-01 V3 y en el Manual de Políticas de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V2 en el numeral 6.48. Gestión de Incidentes de Seguridad de la Información – Ref.: ISO/IEC 27001:2013 CL. A.16.1.

El HOMIL mantiene los contactos apropiados con las autoridades pertinentes y en lo definido por la Resolución 500 de 2021 ARTÍCULO 9. Gestión de incidentes de seguridad digital.

MANUAL	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CODIGO	GT-UNIN-MN-03	VERSION	01
		Página:		35 de 38	

6. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Niveles de seguridad física que se asignará al equipamiento tercerizado.
- Derecho a la auditoría por parte del Hospital Militar Central.

6.48. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN – Ref.: ISO/IEC 27001:2013 CL. A.16.1

a. Los funcionarios, contratistas y terceras partes del Hospital Militar Central deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

b. Para gestionar los incidentes de seguridad de la información deberá existir como mínimo un funcionario con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la información.

c. Los incidentes reportados de mayor complejidad o que no puedan ser solucionados, deberán ser escalados a los CSIRT del Sector Defensa.

d. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.

e. Se debe llevar un registro detallado de los incidentes de seguridad de la información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

f. El Área de Seguridad de la Información debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de seguridad de la información.

g. El Hospital Militar Central deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información.

Fuente: Manual de Políticas de Seguridad y Privacidad de la Información HOMIL

6.11.2 Criterio

CONTINUACIÓN DE LA RESOLUCIÓN NUMERO 00500 DE MARZO 10 DE 2021 HOJA No. 4

"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"

ARTÍCULO 8. *Controles e interoperabilidad.* Los sujetos obligados deben implementar controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura y cumpliendo de los lineamientos dados sobre el particular en el marco de la política de gobierno digital.

ARTÍCULO 9. *Gestión de incidentes de seguridad digital*. Los sujetos obligados deben establecer un procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de cada proceso, para lo cual deben:

1. Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos.
2. Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital.
3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno.
4. Los incidentes catalogados por el responsable de seguridad digital de la entidad, como Menos Grave y Menor, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.
5. Los sujetos obligados, según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.

Fuente: Resolución 500 de Marzo 10 de 2021 MinTIC

6.11.3 Recomendación

Seguir con la ejecución de acuerdo a los tiempos de respuesta establecidos en el GT-GERE-DI-01 catálogo de servicios de incidentes reportados dentro del procedimiento Gestión de Incidentes y Requerimientos PT-GERE-PR-01 V3; así como los tiempos de cierre a fin de minimizar el impacto en las operaciones del Hospital Militar Central.

6.12 Protocolo de políticas de acceso remoto

6.12.1 Condición

No se evidenció un protocolo y políticas de acceso remoto de acuerdo a la directriz impartida por la Presidencia de la República en su Directiva Presidencial No. 02 de 2022.

En el Manual de Políticas de Seguridad y Privacidad de la Información GT-UNIN-MN-03 V1 en su numeral 6, hace mención a los Canales de conexión de acceso remoto de manera general, situación que no permitiría escalar privilegios y mitigar el riesgo de acceso no autorizado a recursos o información:

MANUAL	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CODIGO	GT-UNIN-MN-03	VERSION	01
		Página:		5 de 38	

6. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

sus hogares en situaciones ocasionales, excepcionales o especiales.

b. Esta política será aplicada para funcionarios que acrediten condiciones de salud que les impida cumplir con sus obligaciones en las instalaciones del Hospital Militar Central. Esta situación debe ser avalada previamente por el área de seguridad y salud en el trabajo.

c. El análisis para el aval lo realizará el supervisor inmediato del funcionario, y quien deberá comunicarlo posteriormente a las instancias superiores para la respectiva aprobación

d. La Unidad de Informática debe brindar el acceso a las herramientas tecnológicas que el funcionario requiera para cumplir sus labores según el correspondiente perfil del cargo. Garantizando la seguridad de la información a la cual está ingresando el funcionario.

e. La Unidad de Informática debe garantizar un canal de conexión de acceso remoto (uso de VPN) a los sistemas informáticos del Hospital Militar Central.

f. Se recomienda que los equipos personales de los funcionarios que sean usados para la conexión remota cuenten con antivirus, sistema operativo y programa de ofimática con las actualizaciones de seguridad respectivas.

Fuente: Manual de Políticas de Seguridad y Privacidad de la Información-HOMIL

6.12.2 Criterio

02

IVÁN DUQUE MÁRQUEZ
PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

administren infraestructuras internas o se acceda a servicios misionales internos desde dispositivos no corporativos.

17. Mantener actualizados los sistemas operativos, navegadores, manejador de contenidos, librerías y, en general, todo el software, con las respectivas actualizaciones de seguridad liberadas por los fabricantes.

18. Implementar protocolos y políticas de acceso remoto que eviten a los usuarios escalar privilegios y mitigue el riesgo de acceso no autorizado a recursos o información.

Fuente: Directiva Presidencial 02 de 2022

6.12.3 Recomendación

Mantener actualizada la política de acceso remoto con sus respectivas directrices, autorizaciones y formatos.

7. PQRSDF

Con corte a 19 de octubre del 2023 se radicaron 14 solicitudes por los grupos de interés para el Área de Informática correspondiente a un 0.19% del total de solicitudes radicadas en el HOMIL y estas fueron clasificadas de acuerdo al procedimiento interno así:

Tipo de Solicitud	CANT
Petición	**11**
Reclamo	**3**
TOTAL	**14**

Fuente: Información suministrada por el Área de Atención al Usuario (AUIS)

El comportamiento mensual de PQRSDF recibidas en el área de Informática evidenció mes a mes, a continuación se relacionan:

INFORMATICA	
MESES	**CANT.**
Enero	1
Abril	2
Junio	1
Julio	3
Agosto	5
Septiembre	2
TOTAL	**14**

Fuente: Información suministrada por el Área de Atención al Usuario (AUIS).

1. Dentro de las solicitudes interpuestas por los grupos de valor al área de Informática están relacionadas con recuperación de contraseña en un 42,8%, pagina no funciona 21,42%, solicitud de información 21,42%, falla en dinámica 7,14% y como registrarse en la página web 7,14%.

2. Se resalta que, durante el periodo evaluado, no se presentan solicitudes sin respuesta. Así mismo, no se observó peticiones fuera de término. Teniendo en cuenta los quince (15) días para la respuesta de las PQRSDF establecidos en el Artículo 14 de la Ley 1755/15; se observa un cumplimiento.

8. Matriz de Riesgos Institucional vigencia 2023

Durante el 2 semestre no se materializó ningún riesgo en la Unidad de Informática.

MATRIZ DE RIESGOS INSTITUCIONALES UNIDAD DE INFORMÁTICA

NO. RIESGO	DETALLE RIESGO	CONTROLES
1	Posibilidad de afectación económica y reputacional por registro inoportuno en la Historia Clínica del estado de salud y la atención brindada, debido a la interrupción en la prestación de los servicios tecnológicos de la entidad.	El líder del área de Infraestructura y Comunicaciones - INCO realiza el monitoreo 7*24*365 a través de las herramientas automatizadas de monitoreo (Network Operations Center - NOC) con el fin de verificar el funcionamiento y el estado general de la infraestructura de redes y comunicaciones de la entidad para tomar acciones preventivas y/o correctivas.
		El líder del área de gestión de requerimientos e incidentes - GERE coordina y lidera el comité de cambios conforme el procedimiento (GT-UNIN-PR-01) cada vez que se requiere un cambio de configuración en la infraestructura de redes y comunicaciones; se proyecta el minutograma y las actividades relacionadas con la ejecución del cambio en la infraestructura de redes y comunicaciones que soporta los servicios tecnológicos de la entidad, a través de los formatos establecidos. Con el fin de planear e identificar los impactos que se puedan llegar a generar durante la ejecución.
		El área de Infraestructura y Comunicaciones - INCO, al menos una vez al año realiza un mantenimiento preventivo a la infraestructura de redes y comunicaciones que soporta los servicios tecnológicos, con el fin de asegurar el funcionamiento adecuado de la misma.
		El líder de la Mesa de Servicio de TI - MSTI, cada vez que se requiera realiza los mantenimientos correctivos conforme al procedimiento (GT-GERE-PR-01) a los equipos de cómputo de los diferentes servicios asistenciales, con el fin de asegurar el funcionamiento adecuado de los mismos.
2	Posibilidad de afectación reputacional y perdida de la confidencialidad por el acceso a información clasificada o reservada de los usuarios del Homil, debido a falta de control del ciclo de vida de las credenciales de acceso a la infraestructura tecnológica de la entidad.	El área de gestión de seguridad informática - GESU, mensualmente realiza campañas de sensibilización en temas de ciber seguridad. Con el fin de concientizar a los usuarios de los riesgos relacionados con el uso seguro de la infraestructura tecnológica que soporta la prestación de los servicios tecnológicos.
		El área de Gestión de Movilidad y Aplicaciones - GEAM informa mensualmente a los jefes de Unidad los usuarios activos en el sistema de Información Dinámica gerencial para recibir retroalimentación de la permanencia en los cargos de los profesionales de la salud.
		El área de Mesa de Servicio de TI - MSTI, solo crea las cuentas de acceso a las personas que alleguen 100% diligenciado el formato único de solicitud de acceso a servicios informáticos (TI-GESU-PR-01-FT-01)
		La Unidad de Talento Humano, reporta vía correo electrónico las novedades de personal (retiros) a fin de que se deshabiliten los accesos a los diferentes servicios tecnológicos.
		El área de Mesa de Servicio de TI - MSTI, configura la fecha de terminación del contrato relacionada en el formato único de solicitud de acceso a servicios informáticos (TI-GESU-PR-01-FT-01). Está configuración se realiza en el directorio activo para que se bloquee de manera automática el día que corresponda.
		El administrador de la base de datos del área de infraestructura y comunicaciones - INCO configura un script automático para deshabilitar usuarios que lleven más de un mes sin ingresar al sistema de información Dinámica Gerencial.
3	Posibilidad de afectación económica por no disponibilidad de la información clínica de los usuarios del HOMIL, debido a falta de respaldo (copias de seguridad) de la información.	El líder del área de Infraestructura y Comunicaciones - INCO realiza el monitoreo 7*24*365 a través de las herramientas de monitoreo (NOC) con el fin de verificar el funcionamiento y el estado general de los equipos que soportan el servicio de backup de la entidad para tomar acciones preventivas y/o correctivas.
		El administrador de la base de datos del área de infraestructura y comunicaciones, verifica el log de eventos en la herramienta de backup de la entidad que indique la realización y terminación correcta de copias de datos. Con el fin de asegurarse que se tiene una copia de respaldo consistente y disponible para cuando se necesite.
4	Posibilidad de afectación económica y reputacional por fallas en el funcionamiento del sistema de información clínico Dinámica Gerencial Hospitalaria generadas por el indebido control de cambios en la implementación de nuevas versiones del aplicativo.	Los líderes de módulos del aplicativo Dinámica Gerencial Hospitalaria del área de Gestión de requerimientos e incidentes - GERE, coordinan y lideran el comité de cambios conforme al procedimiento (GT-UNIN-PR-01) cada vez que se requiere un cambio en el aplicativo Dinámica Gerencial Hospitalaria; en el escenario de pruebas de la aplicación las actividades relacionadas en el protocolo de pruebas de nueva compilación, el cual incluye las pruebas técnicas realizadas por los líderes funcionales de cada proceso y el funcionamiento de las opciones de los diferentes módulos, en conjunto con los líderes funcionales en cada proceso; lo anterior con el fin de validar si estas tuvieron cambios de funcionamiento y/o funcionan de manera adecuada.
		El líder de la mesa de servicio TI de la Unidad Informática, una vez finalizada la actualización de la nueva versión de Dinámica Gerencial Hospitalaria, iniciará un recorrido preventivo por las áreasasistenciales (Desde el piso 12, hasta urgencias y salas de cirugía); revisando la funcionalidad y operatividad del sistema de información. El personal encargado del recorrido firmará la bitacora de recorridos de la UNIN.

Fuente: Matriz de Riesgos Institucionales 2023 V2– HOMIL

8.1 Recomendación

La OCIN recomienda continuar con la ejecución de los controles para mitigar los riesgos identificados por la Unidad de Informática, evaluando su efectividad de forma periódica y posible materialización.

9. CONCLUSIONES

- Se pudo evidenciar grandes avances en el proceso de implementación del MSPI; a la fecha se ha logrado evaluar y analizar la construcción de los lineamientos establecidos por la MINTIC y MINDEFENSA para su adecuada implementación en la entidad.

  Así mismo, se ha visto la evolución en su construcción e implementación de los controles tecnológicos que abarcan todos los dominios del modelo. Sin embargo, queda por perfeccionar los mecanismos para medir técnicamente la efectividad de los controles y la toma de acciones correctivas, de acuerdo con las recomendaciones presentadas en este informe.

- El proceso de implementación del MSPI se encuentra aún en etapa de ejecución, lo que permite realizar ajustes y adecuaciones efectivas en pro al cumplimiento de las obligaciones, responsabilidades, lineamientos y políticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Ministerio de Defensa.

- No existe un equipo de trabajo enfocado al Modelo de privacidad y seguridad de la información que permita implementar un sistema con los lineamientos mínimos como lo indica el MINTIC en cada una de sus guías, dado que la única persona que lidera el proceso es la misma que lidera la Unidad de Informática de toda la entidad; sin embargo se ha logrado avanzar en la materia alcanzando un nivel de madurez del Modelo importante como se pudo evidenciar en el presente informe.

- No se presentaron limitaciones durante el ejercicio de la actividad, se reconoce la colaboración del responsable de la Unidad de Informática, lo que facilitó la comprensión de la información presentada en procura de conocer el trabajo realizado en el marco del objetivo del seguimiento.

- Se hizo seguimiento de evaluación al diseño, implementación y ejecución de los controles, 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 en la normatividad vigente

- La Matriz de Riesgos Institucional vigencia 2023 V2, demuestra que se viene avanzando en la identificación de riesgos y controles; sin embargo se debe fortalecer el ejercicio aplicando metodología vigente de la administración de riesgos existentes en los procesos existentes. Lo anterior con el fin de cubrir los diferentes tipos de activos de información (información, software, hardware, componentes de red, servicios intangibles, personas e instalaciones) que afecten el desempeño del HOMIL en las dimensiones de integridad, disponibilidad y confidencialidad.

EVIDENCIAS	CANTIDAD
HALLAZGOS	2
RECOMENDACIONES	22

10. RECOMENDACIONES

- Realizar revisión periódica de las categorías de activos de información, propiedades y criterios de valoración, con el fin de definir los activos críticos de la entidad y entendimiento de la aplicabilidad de los controles y análisis de riesgos de los diferentes grupos de activos.
- Sensibilizar a los empleados y contratistas para tomar conciencia de su responsabilidad frente al reporte de eventos de seguridad de la información.
- Continuar con las comunicaciones a los usuarios, generar campañas y espacios para fomentar el reporte de incidentes, debilidades de seguridad de la información con su correspondiente análisis de causas que lo ocasionan, permitiendo así una mejor toma de decisiones.
- Llevar control de los riesgos de seguridad digital consolidado con el fin de establecer un seguimiento a los planes de mejora, registro de materialización de riesgos y actualización de la matriz de riesgos institucionales catalogados con tipología de corrupción y de gestión.
- Se recomienda fortalecer y mantener el equipo de trabajo para la implementación de la Política de Gobierno Digital en el HOMIL; incluyendo el personal necesario para implementar el Modelo de Privacidad y Seguridad de la Información (MSPI).
- Se sugiere formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información; además de contemplar su papel dentro de los procesos transversales a la entidad.
- Se recomienda que en las campañas se pueda diferenciar fácilmente los términos de seguridad digital, seguridad de la información y seguridad informática para todos los miembros de la entidad, con el fin de poder reconocer sus responsabilidades y alcances en el proceso.
- Se recomienda el diseño de procedimientos e inclusión de controles de acuerdo a los nuevos lineamientos de la ISO/IEC 27001:2022:

Sandra Milena Oliveros S
Auditora Contadora Especialista OPS