| Fecha emisión del informe | día | 20 | mes | 08 | año | 2020 |
|---|---|---|---|---|---|---|

| | |
|---|---|
| **Proceso:** | Gestión TIC |
| **Procedimiento/operaciones.** | Cumplimiento normativo |
| **Líder de Proceso: Jefe(s) Dependencia(s):** | Fernando Ramírez Ochoa - Director Financiero y Administrativo<br>Cesar Ortiz Responsable del Proceso TIC |
| **Nombre del seguimiento:** | Seguimiento implementación del Sistema de Gestión de Seguridad de la Información y Mapa de Riesgos de Seguridad Digital. |
| **Objetivo:** | Evaluar el estado de avance de proyecto de implementación del Sistema de Gestión de Seguridad de la Información SGSI y la Gestión de Riesgos de Seguridad Digital. |
| **Metodología** | El seguimiento se realizó atendiendo los procedimientos vigentes establecidos en el Sistema Integrado de Gestión, así como la normatividad aplicable, efectuándose levantamiento de información, reuniones virtuales de validación de la información. El seguimiento fue realizado entre el 2 junio y 28 de julio.<br><br>Este seguimiento está conformado por dos informes: el presente con alcance al SGSI y otro informe con alcance al Mapa de Riesgos de Seguridad Digital |
| **Limitaciones o riesgos del proceso de seguimiento** | Se realizó la verificación de la información dispuesta virtualmente por el líder del proceso, no se tuvo acceso a información en físico o verificaciones en campo debido a las restricciones generadas por la emergencia sanitaría |

| Asesor de Control Interno | Equipo Evaluador de control interno |
|---|---|
| Doris Yolanda Ramos Vega | José Edgar Hernando Galarza Bogotá |

## DESARROLLO DEL SEGUIMIENTO
## (Temas evaluados – Conclusiones)

### 1. Justificación

Con la expedición del Decreto 1499 de 2017 (cuyas disposiciones fueron compiladas en el Decreto Único Reglamentario del Sector Función Pública 1083 de 2015, Título 22, Parte 2 del Libro 2), el Departamento Administrativo de la Función Pública, reglamentó el Sistema Integrado de Planeación y Gestión y actualizó el modelo para su implementación, denominado "Modelo Integrado de Planeación y Gestión –MIPG", que consiste en un "marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio"1 .

A partir de lo anterior, Gobierno Digital es una de las diecisiete políticas de gestión y desempeño institucional, que se desarrolla en el marco del Modelo Integrado de Planeación y Gestión y se encuentra en el Eje de Gestión

para el Resultado con Valores.

Dada la transversalidad de los medios digitales en los procesos internos de la entidad y en el relacionamiento con los usuarios, la Política de Gobierno Digital está estrechamente relacionada con las políticas de: Planeación Institucional, Talento humano, Transparencia, Acceso a la Información Pública y Lucha Contra la Corrupción, Fortalecimiento Organizacional y Simplificación de Procesos, Servicio al Ciudadano, Participación Ciudadana en la Gestión Pública, Racionalización de trámites, Gestión Documental, Seguridad Digital y Gestión del Conocimiento y la Innovación.

La Política de Gobierno Digital tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".

La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores, que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano, a través de la participación y la prestación de servicios de calidad.

*La evolución de la política no implica que las entidades públicas que venían implementando la Estrategia de Gobierno en Línea, deban comenzar desde cero, pues la Política de Gobierno Digital da continuidad a los temas que se venían trabajando desde la Estrategia de Gobierno en Línea*.

El documento conocido tradicionalmente como "Manual de Gobierno en Línea" y que evolucionó para ser el "Manual para la implementación de la política de Gobierno Digital", se encuentra incorporado en el artículo 2.2.9.1.2.2. del Decreto Único Reglamentario del Sector TIC, en donde se estable:

"ARTÍCULO 2.2.9.1.2.2 Manual de Gobierno Digital. Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación."

En este sentido, el Manual de Gobierno Digital desarrolla el proceso de implementación de la política a través de cuatro grandes momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política, los cuales incorporan las acciones que permitirán desarrollar la política en las entidades públicas de nivel nacional y territorial.

Para la implementación de la Política de Gobierno Digital, se han definido dos componentes: TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información,

Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos se desarrollan a través de lineamientos y estándares2, que son los requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

Los componentes TIC para el Estado y TIC para la Sociedad son líneas de acción que orientan el desarrollo y la implementación de la política.

Los habilitadores transversales Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, son elementos fundamentales que permiten el desarrollo de los componentes de la política.

EL habilitador transversal Seguridad de la información, busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información -MSPI, que contempla 6 niveles de madurez.

**EJECUTORES DE LA POLITICA DE GOBIERNO DIGITAL**

La política de Gobierno Digital tiene como ámbito de aplicación, las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política (Art. 2.2.9.1.1.2. - Decreto 1078 de 2015).

Así mismo, con el objetivo de identificar claramente los roles para la implementación de la Política de Gobierno Digital, se define un esquema institucional que vincula desde la alta dirección hasta las áreas específicas de la entidad en el desarrollo de la política y el logro de sus propósitos. A continuación, se presentan estas instancias y sus responsables de la implementación de la política:

MINTIC: Líder de la política de Gobierno Digital: es el Ministerio de Tecnologías de la Información y las Comunicaciones, quién a través de la Dirección de Gobierno Digital, se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial.

REPRESENTANTE LEGAL DE LA ENTIDAD: Responsable Institucional de la Política de Gobierno Digital: es el representante legal de cada sujeto obligado y es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital.

Como responsables de la política de Gobierno Digital, los representantes legales (ministros, directores, gobernadores y alcaldes, entre otros), deben garantizar el desarrollo integral de la política como una herramienta transversal que apoya la gestión de la entidad y el desarrollo de las políticas de gestión y desempeño

institucional del Modelo Integrado de Planeación y gestión.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO: Responsable de orientar la implementación de la Política de Gobierno Digital: es el Comité Institucional de Gestión y Desempeño, de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015. Esta instancia será la responsable de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Teniendo en cuenta que la principal función de este comité es orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra Gobierno Digital), esta instancia debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad.

LÍDER TIC: Responsable de liderar la implementación la Política de Gobierno Digital: es el director, jefe de oficina o coordinador de tecnologías y sistemas de la información y las comunicaciones o G-CIO (sigla en inglés de Government Chief Information Officer), o quien haga sus veces en la entidad, de acuerdo con el artículo 2.2.35.5. del Decreto 1083 de 2015. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

El director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo con lo establecido en el artículo 2.2.35.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.

Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología como una herramienta que habilita la gestión de la entidad para la generación de valor público, todas las áreas o dependencias son corresponsables en su implementación.

LIDER SEGURIDAD DE INFORMACION: Atendiendo a la necesidad de articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación de las políticas en materia de Seguridad de la Información, incluyendo la Seguridad Digital, en la respectiva entidad, se debe designar un Responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección (MIPG, 2017).

El Responsable de Seguridad de la información será el líder del proyecto, escogido dentro del equipo designado en cada entidad y tendrá las responsabilidades establecidas en la guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (Guía 4 - Roles y Responsabilidades), quien, a su vez, tiene responsabilidades asignadas dentro de cada dominio del Marco de Arquitectura Empresarial. El responsable de seguridad de la información deberá participar en los comités de desempeño institucional.

Así mismo, el responsable de seguridad de la información debe apoyar a los líderes de los procesos o áreas de

la entidad, con el objetivo de implementar adecuadamente los lineamientos, esto incluye la identificación de los activos y los riesgos derivados en estos.
De igual manera, el responsable de seguridad de la información se debe apoyar fundamentalmente en el CIO de la entidad para mitigar los riesgos asociados a la tecnología (Seguridad Informática o Ciberseguridad), también se debe apoyar en otras áreas que permitan mitigar otros tipos de riesgos de seguridad de la información, Ej. Recursos Físicos, Talento Humano entre otras.

NOTA: Para lograr un adecuado balance entre funcionalidad y seguridad, se recomienda que el elemento transversal de seguridad de la información opere de manera independiente a la Oficina de T.I. En este caso, la entidad puede ubicar esta iniciativa en un área como planeación, procesos, el área relacionada con gestión de riesgos, o bien, crear una nueva área dedicada a la seguridad de la información.

CONTROL INTERNO: De acuerdo con lo definido en la Dimensión 7 de Control Interno del Modelo Integrado de Planeación y Gestión, las oficinas de control interno desempeñan un rol específico en materia de control y gestión del riesgo, con el fin de apoyar el desarrollo de un adecuado ambiente de control, una efectiva gestión del riesgo, la implementación de controles efectivos y un monitoreo y supervisión continua a la gestión de la entidad. En este sentido, la alta dirección, los líderes de proceso y los servidores públicos relacionados con la implementación de Gobierno Digital, deben articular con la oficina de control interno el desarrollo de acciones, métodos y procedimientos de control y de gestión del riesgo para la implementación de la política.

Control Interno adelantó el seguimiento mediante el levantamiento de información, entrevistas y validación de la información disponible, con el fin de evidenciar el avance en la implementación de los controles del Sistema de Gestión de Seguridad de la Información. Durante el periodo de seguimiento, se pudo establecer lo siguiente:

El CNMH estableció el Plan Operacional Seguridad y Privacidad de la información con base en el cual durante la vigencia 2019 inicio la actualización del SGSI, dentro de las actividades más relevantes adelantadas se evidenció la actualización del documento de Políticas del Seguridad de Información, la aprobación del mismo por parte del Comité Institucional de Gestión y Desempeño, la actualización del inventario de activos de información al igual que se adelantaron actividades de sensibilización y socialización del Sistema. Lo anterior se logró principalmente a la contratación de un profesional con la idoneidad y experiencia requeridas para apoyar la gestión del SGSI.

Para el 2020 el CNMH planeó la sostenibilidad del SGSI y la actualización e implementación de los controles del Modelo de Seguridad y Privacidad de información pertinentes. Se evidencia que en lo corrido de la vigencia 2020 las actividades planeadas se han visto limitadas en su oportunidad y alcance teniendo en cuenta que la DAYF ya no cuenta con recursos humanos especializados en el tema. *Por lo anterior se recomienda se revisé la oportunidad y conveniencia de fortalecer la gestión para asegurar la sostenibilidad del SGSI.*

A continuación, se describe el estado de avance en la implementación de los controles de SGSI con base en el modelo de Seguridad y Privacidad de la Información establecido por el MINTIC.

**CONTROLES DOMINIO 5. POLÍTICA DE SEGURIDAD**

Este Dominio establece como objetivo de control 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

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

5.1.1 Políticas para la seguridad de la información: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

En el seguimiento se evidenció que la Entidad cuenta con el instrumento SIP- PC-013 Política de Seguridad de Información en el SGSI y publicada en la Intranet en noviembre de 2017, dicha política se adoptó mediante la Resolución Interna 206 de 23 de julio de 2018. Durante la vigencia 2019 el Comité Institucional de Gestión y Desempeño revisó y aprobó las Políticas.
Se evidencia que la Política fue socializada en 2019 a los servidores públicos del CNMH, sin embargo no se evidencia que se hayan realizado socializaciones o capacitaciones durante la vigencia del 2020 y tampoco se evidencia su socialización a partes externas como son proveedores. Se recomienda fortalecer las actividades de socialización y capacitación a nivel interno y externo, en especial a proveedores del CNMH

5.1.2 Revisión de las políticas para seguridad de la información: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.

Se evidencia que en el artículo segundo de la Resolución 206 de 2018 se establece que la Política de Seguridad debe revisarse con periodicidad al menos anual, por parte del Comité Institucional de Gestión y Desempeño. En lo corrido de la vigencia 2020 no se han realizado revisiones de la Política de SGSI, se recomienda que se programe dicha revisión en la agenda del Comité.

**ARTÍCULO SEGUNDO. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.** El Comité Institucional de Gestión y Desempeño será el responsable de realizar las revisiones de la Política de Seguridad de la Información y lo hará al menos una vez al año o cuando ocurran cambios en el entorno organizacional, marco legal o ambiente técnico.

De acuerdo con lo establecido en el Artículo Tercero de la Resolución 206 de 2018 y en el Artículo Décimo Cuarto de la Resolución 038 del 31 de enero de 2018, No se evidencia que en los Comités Institucionales de Gestión y Desempeño celebrados durante 2020 se haya presentado por parte del *líder de Seguridad* de Información del CNMH el estado de avance de la implementación del SGSI, adicionalmente no se evidencia que el Comité haya hecho seguimiento a las acciones para la implementación de los controles del SGSI. Por lo

anterior se recomienda que se incluya en la agenda del Comité Institucional de Gestión y Desempeño el seguimiento al estado del SGSI.

**CONTROLES DOMINIO 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

Este Dominio establece dos (2) objetivos de control

6.1 Organización Interna: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

6.1.1 Roles y responsabilidades para la seguridad de información: Se deberían definir y asignar todas las Responsabilidades de la seguridad de la información.

Se evidencia que en el numeral 6. ESTRUCTURA ORGANIZACIONAL del documento: SIP-MA-002 Manual Sistema Gestión Seguridad Información, se establecen responsabilidades para la seguridad de la información. Adicionalmente recomienda la creación del Rol de OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.

Sin embargo, a la fecha no se evidencia que el CNMH haya nombrado y asignado las funciones específicas para el rol de Oficial de Seguridad de la Información de acuerdo con lo definido en el Manual de SGSI. Se recomienda se revisé la asignación del Rol de Oficial de Seguridad de Información y se establezcan formalmente la funciones correspondientes-

Adicionalmente La Resolución Interna 206 de 23 de julio de 2018 modifica la Resolución 038 de 31 de enero de 2018, adicionando funciones de seguridad de la información al Comité Institucional de Gestión y Desempeño. Con base en lo anterior no se evidencia en las actas de la vigencia 2020 que el Comité haya tomado las decisiones pertinentes para asegurar la implementación, sostenibilidad y mejora del SGSI.

6.1.2 Separación de deberes: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

No se evidencia la implementación del control.

6.1.3 Contacto con las autoridades: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
6.1.4 Contacto con grupos de interés especial: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

Se evidencia un registro del funcionarios Cesar Ortiz en la página de la Cámara Colombiana de Informática y Telecomunicaciones CCIT, sin embargo no se evidencia la existencia de un control formal y documentado que aseguré su efectividad.

6.1.5 Seguridad de la información en la gestión de proyectos: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto

No se evidencia la existencia de un control formal que asegure la efectividad y sostenibilidad del mismo en la gestión de proyectos del CNMH

6.2 Dispositivos móviles y Teletrabajo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

6.2.1 Política para dispositivos móviles: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

Se evidencia que el CNMH implementó el control mediante la política SIP-PC-004 V1 Política de dispositivos móviles aprobada el 05/08/2016, sin embargo no se evidencia que se esté aplicando ya que no se tiene evidencia física o electrónica de los registros de los documentos de los “Acuerdos de Uso” y la revisión periódica de los mismos.

6.2.2 Teletrabajo: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Se evidencia que el CNMH definió y formalizó el control mediante la política SIP-PC-010-Política de teletrabajo, aprobada y publicada en la intranet-SGI, sin embargo, no se evidencia que se esté aplicando. Por lineamientos del Gobierno Nacional el CNMH está aplicando el trabajo en casa el cual genera nuevos riesgos en las variables de la información. Por lo anterior se recomienda realizar el análisis de riesgo de esta modalidad de trabajo y se defina el tratamiento de los mismos.

**CONTROLES DOMINIO 7. SEGURIDAD DE LOS RECURSOS HUMANOS**

Este Dominio establece dos (2) objetivos de control

7.1 Antes de Asumir el empleo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y su idoneidad en los roles para los que se consideran

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

7.1.1 Selección: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

Se evidencia que el CNMH implementó el control mediante el procedimiento GTH-PR-002 V4 Vinculación de Talento Humano y los formatos "ABS-FT-007 V8 Lista de Chequeo - Personas Naturales y GTH-FT-040 V1Compromiso de confidencialidad y protección de información.

7.1.2 Términos y condiciones del empleo: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

Se evidencia que el CNMH implementó el control mediante el formato ABS-FT-013 V6 Minuta de Contrato de Prestación de Servicios Profesionales y de Apoyo a la Gestión, la cual contiene en su clausulado de obligaciones respecto de la seguridad y confidencialidad de la información. Adicionalmente la Dirección de Archivo de Derechos Humanos gestionó la firma de un acurdo de confidencialidad para todos los funcionarios del área.

7.2 Durante la ejecución del empleo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

7.2.1 Responsabilidades de la dirección:" La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización"

Se evidencia que el CNHM cuenta con la implementación del SGSI como parte del Sistema Integrado de Gestión y cuenta con la Resolución 306 de 2018 que adopta las políticas de seguridad de Información.

7.2.2 Toma de conciencia, educación y formación en la seguridad de la información: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo

Se evidencia que en lo corrido de la vigencia de 2020 la DAYF no han realizado actividades de capacitación para los servidores públicos de la Entidad en materia de Seguridad de Información. Se recomienda fortalecer el

proceso de socialización y capacitación para el segundo semestre de 2020 y la vigencia 2021.

7.2.3 Procesos disciplinarios: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Se evidencia que el CNHM cuenta con proceso y procedimientos para el Control Disciplinario para la gestión de faltas de los funcionarios de planta los cuales aplican para los casos de incidentes de la Seguridad de la Información. No se evidencia que en lo corrido de la vigencia 2020 se hayan adelantado procesos disciplinarios por incumplimiento de las políticas de seguridad de la información.

7.3 Terminación del contrato o cambio del empleo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece el siguiente control:

7.3.1. Terminación o cambio de responsabilidades de empleo: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.

Se evidencia que el CNHM cuenta con un compromiso de confidencialidad y protección de la información, donde el incumplimiento del mismo puede conllevar a sanciones disciplinarias y/o penales a que haya lugar. Así mismo, entiende que las condiciones indicadas, pueden ser extensibles incluso después a la cesación de los servicios y/o actividades.

**CONTROLES DOMINIO 8. GESTIÓN DE ACTIVOS**

Este Dominio establece tres (3) objetivos de control

8.1 Responsabilidad de Activos: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

8.1.1 Inventario de activos: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Se evidencia que el CNHM cuenta cuenta con un inventario de activos revisado y aprobado por la Dirección, cuya última fecha de actualización fue a finales de 2019, adicionalmente el SGSI cuenta una metodología de

clasificación de Activos y un procedimiento de clasificación de activos-SIP-PR-016.

8.1.2 Propiedad de los activos: Los activos mantenidos en el inventario deberían tener un propietario.

Se evidencia que el CNHM inventario de activos de información de la DADH contiene la relación de los activos de información y sus propietarios, la fecha de última fue a finales de 2019

8.1.3 Uso aceptable de los activos tecnológicos: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Se evidencia que el CNMH implementó el control mediante el Documento de la Metodología de Clasificación de activos y Documento de Compromiso de confidencialidad y protección de la información.

8.1.4 Devolución de activos: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo

Se evidencia que el CNMH implementó el control mediante el formato GRF-FT-002 V2 -Devolución de bienes en servicio, Adicionalmente en el Manual de administración de los recursos físicos.

8.2. Clasificación de la información: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

8.2.1 Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o la modificación no autorizada.

Se evidencia que el CNHM cuenta cuentan con una metodología de clasificación de Activos y un procedimiento de clasificación de activos-SIP-PR-016. .

8.2.2 Etiquetado de la información: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Se evidencia que el CNMH implementó el control mediante el procedimiento SIP-PR-011 V1 Etiquetado_de_Información. Sin embargo, no se tiene evidencia de que el control se esté aplicando en la DADH de acuerdo a los establecido en dicho procedimiento, ya que no se suministró el etiquetado de los activos de información igualmente no fueron suministrados los formatos SIP-FT-013 debidamente diligenciados.

8.2.3 Manejo de activos: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Se evidenció que el CNMH implementó el control mediante el documento "Metodología de Clasificación de activos" y con el documento "Compromiso de confidencialidad y protección de la información".

8.3. Manejo de los Soportes de Almacenamiento

8.3.1. Gestión de medios removibles: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

Se evidencia que el CNMH implementó el control mediante el procedimiento SIP-PR-013 V1 Gestión de medios removibles, sin embargo no se obtuvo evidencia de su aplicación mediante los registros establecidos en la actividad 9-Resgistro de Gestión de dicho procedimiento.

8.3.2 Disposición de los medios: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales

Se evidencia que el CNMH no ha implementado formalmente este control en el SGSI

8.3.3 Transferencia de medios físicos: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Se evidencia que el CNMH implementó el control mediante el procedimiento SIP-PT-001 Protocolo de intercambio seguro de información el cual fue actualizado en la vigencia 2019.

**CONTROLES DOMINIO 9. CONTROL DE ACCESO A LA INFORMACIÓN**

Este Dominio establece cuatro (4) objetivos de control,

9.1 Requisitos del negocio para control de acceso: Limitar el acceso a información y a instalaciones de Procesamiento de información.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

9.1.1 Política de Control de Acceso: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Se evidencia que el CNMH en el Artículo Octavo del Documento SIP-PC-013 Políticas de Seguridad de

Información se contempla la Política de Control de Acceso a la Información.

9.1.2 Política sobre el uso de los servicios de red: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

Se evidencia que el CNMH implementó el control mediante el procedimiento SIP-PR-008. Registro y cancelación de cuentas de usuario y en la Política de uso aceptable de los recursos informáticos inmersa en SIP-PC-013.

9.2 Gestión de acceso de los usuarios: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

Para el cumplimiento del objetivo el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

9.2.1 Registro y cancelación del registro de usuarios: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2 Suministro de acceso de usuarios: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios
9.2.3 Gestión de derechos de acceso privilegiado: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
9.2.4 Gestión de información de autenticación secreta de usuarios: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
9.2.5 Revisión de los derechos de acceso de usuarios: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.

Se evidencia que el CNMH implementó el control mediante el procedimiento SIP-PR-008. Registro y cancelación de cuentas de usuario. V1. Sin embargo, se evidenció que la gestión de acceso a los sistemas de información no se aplican los controles establecidos. *La descentralización de la operación del módulo de seguridad de los diferentes sistemas de Información genera debilidad en el control de acceso.*

9.3 Responsabilidades de los usuarios Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

9.3.1 Uso de la información de autenticación secreta Control: Se debería exigir a los usuarios que cumplan las prácticas de la entidad para el uso de información de autenticación secreta.

9.4 Control de acceso a sistemas y aplicaciones Objetivo: Evitar el acceso no autorizado a sistemas y

aplicaciones.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

9.4.1 Restricción de acceso Información Control: *El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.*
9.4.2 Procedimiento de ingreso seguro Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
9.4.3 Sistema de gestión de contraseñas Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
9.4.4 Uso de programas utilitarios privilegiados Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
9.4.5 Control de acceso a códigos fuente de programas Control: Se debería restringir el acceso a los códigos fuente de los programas.

Se evidencia que los siguientes controles establecidos en este Dominio a la fecha no están implementados:
A.9.2.4 Gestión de información de autenticación secreta de usuarios
A.9.2.5 Revisión de los derechos de acceso de usuarios
A.9.3.1 Uso de la información de autenticación secreta
A.9.4.5 Control de acceso a códigos fuente de programas

**CONTROLES DOMINIO 10 CRIPTOGRAFIA**

Este Dominio establece un (1) objetivo de control,

10.1 Controles criptográficos Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

10.1.1 Política sobre el uso de controles criptográficos Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
10.1.2 Gestión de llaves Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida

El CNMH cuenta con una política implementada de uso de criptografía, adicionalmente se utiliza un software de cifrado para la información que sale del centro en dispositivos de almacenamiento externo, al igual que se utilizan llaves o Tokens para el acceso al sistema de gestión financiera

**CONTROLES DOMINIO 11 SEGURIDAD FISICA Y DEL ENTORNO**

Este Dominio establece dos (2) objetivos de control:

11.1 Áreas seguras Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

11.1.1 Perímetro de seguridad física Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
11.1.2 Controles físicos de entrada Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
11.1.3 Seguridad de oficinas, recintos e instalaciones Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
11.1.4 Protección contra amenazas externas y ambientales Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
11.1.5 Trabajo en áreas seguras Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
11.1.6 Áreas de despacho y carga Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

11.2 Equipos Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

11.2.1 **Ubicación y protección de equipos**: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. 11.2.2 Servicios de suministro Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
11.2.3 Seguridad del cableado Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
11.2.4 Mantenimiento de equipos Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
1.2.5 Retiro de activos Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
11.2.6 Seguridad de equipos y activos fuera de las instalaciones Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
11.2.7 Disposición segura o reutilización de equipos Control: Se deberían verificar todos los elementos de

equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
11.2.8 Equipos de usuario desatendidos Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
11.2.9 Política de escritorio limpio y pantalla limpia Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

*El conjunto de controles de este dominio se encuentra establecidos en el documento de* ***Políticas de Seguridad de la información****, sin embargo, se recomienda actualizar los pertinentes teniendo en cuenta las nuevas condiciones de operación del CNMH motivadas por la emergencia sanitaria. Lo anterior teniendo en cuenta por ejemplo que algunos funcionarios se les ha entregado equipos de cómputo para trabajo remoto*

**CONTROLES DOMINIO 12 SEGURIDAD DE LAS OPERACIONES**

Este Dominio establece siete (7) objetivos de control:

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

12.1 Procedimientos operacionales y responsabilidades
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

12.1.1 Procedimientos de operación documentados Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
12.1.2 Gestión de cambios Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
12.1.3 Gestión de capacidad Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
12.1.4 Separación de los ambientes de desarrollo, pruebas y operación Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación

Se evidencia que los controles 12.1.3 Gestión de capacidad y 12.1.4 Separación de los ambientes de desarrollo, pruebas y operación no se han implementado, sin embargo, el Grupo TIC desarrolló el documento de gestión de capacidad, el cual permitirá contar con el análisis de capacidad actual y las necesidades de corto y mediano plazo. Se recomienda adelantar las actividades necesarias para el diseño, implementación y aplicación de los

controles pendientes.

*Adicionalmente se evidencia que no se cuenta la bitácora de cambios de la plataforma tecnológica para la vigencia 2019 y 2020 tanto a nivel de hardware, software operativo y aplicaciones que soportan los sistemas de información, lo anterior muestra debilidades en la gestión de cambios de la plataforma y generando dificultades al momento contar con información para el análisis de incidentes de seguridad de la información. Lo anterior se materializo con el incidente de seguridad del sistema de gestión documental.*

12.2 Protección contra códigos maliciosos
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece el siguiente control:

12.2.1 Controles contra códigos maliciosos Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Se evidencia que el CNMH ha implementado controles automáticos como el Firewall y Software Antivirus para el control de código malicioso.

12.3 Copias de respaldo
Objetivo: Proteger contra la perdida de datos.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece el siguiente control:

12.3.1 Respaldo de información Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

*Se evidencia que el CNMH cuenta con equipos para efectuar copias de respaldo, al igual que para los servicios contratados externamente se tiene el servicio de copias de respaldo. Sin embargo, se evidencia que no se realizan las pruebas a las copias de respaldo con el fin de asegurar su consistencia y disponibilidad. Se recomienda fortalecer el control de copias de respaldo definiendo la política de pruebas de dichas copias y hacerla extensiva a los contratos con los proveedores correspondientes*.

12.4 Registro y seguimiento
Objetivo: Registrar eventos y generar evidencia.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece el siguiente control:

12.4.1 Registro de eventos Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2 Protección de la información de registro Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
12.4.3 Registros del administrador y del operador Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
12.4.4 sincronización de relojes Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.

*Se evidencia que no se cuenta con la implementación de los controles 12.4.1 Registro de eventos Control, 12.4.2 Protección de la información de registro Control, 12.4.3 Registros del administrador y del operador Control, se recomienda se defina diseñe, implemente y se apliquen los controles pendientes. Adicionalmente se evidenció que el sistema de gestión documental no cuenta con traza de auditoria que permita identificar las actividades del administrador, lo cual genera riesgos de integridad, disponibilidad y confidencialidad de la información.*

12.5 Control de software operacional
Objetivo: Asegurar la integridad de los sistemas operacionales.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece el siguiente control:

12.5.1 Instalación de software en sistemas operativos Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.

12.6 Gestión de la vulnerabilidad técnica
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece el siguiente control:

12.6.1 Gestión de las vulnerabilidades técnicas Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
12.6.2 Restricciones sobre la instalación de software Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios

*Se evidencia que el control 12.6.1 Gestión de las vulnerabilidades técnicas no está implementado y por lo tanto, no se cuenta con información de las vulnerabilidades de la plataforma tecnológica y como consecuencia no se cuenta con actividades para mitigar dichas vulnerabilidades. Se recomienda diseñar, implementar y aplicar controles para realizar el análisis de vulnerabilidad de la plataforma tecnológica del CNMH con carácter prioritario.*

Adicionalmente se evidencia el grupo TIC informa que los servidores que administra la entidad están sincronizados con la plataforma de la hora legal colombiana.

12.7 Consideraciones sobre auditorias de sistemas de información
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.

12.7.1 Información controles de auditoría de sistemas Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio

*Este control a la fecha no se ha implementado.*

**CONTROLES DOMINIO 13 SEGURIDAD DE LAS COMUNICACIONES**

Este Dominio establece dos (2) objetivos de control:

13.1 Gestión de la seguridad de las redes
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

13.1.1 Controles de redes Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
13.1.2 Seguridad de los servicios de red Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente
13.1.3 Separación en las redes Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.

Se evidencia que el CNMH cuenta con el Diseño e implementación de la segmentación de Red en IPv4 e IPv6, se tiene diseñada e implementada la segmentación en varias VLANS de usuarios, de servidores y redes inalámbricas.

13.2 Transferencia de información
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos de transferencia de información Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
13.2.2 Acuerdos sobre transferencia de información Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
13.2.3 Mensajería electrónica Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
13.2.4 Acuerdos de confidencialidad o de no divulgación Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

*Se evidencia que no cuenta con la documentación formal de este grupo de controles, sin embargo, existen controles automáticos como el FireWall que permite filtrar el tráfico para cada servidor, la mensajería electrónica se gestiona de forma segura a través de filtros implementados en el firewall el cual mitiga el riesgo de integridad de la información, adicionalmente se cuenta con software antivirus, el cual protege la mensajería electrónica al interior de la Red LAN. Se recomienda formalizar y documentar las políticas correspondientes y demás documentos necesarios para asegurar la sostenibilidad de los controles.*

**CONTROLES DOMINIO 14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS**

Este Dominio establece dos (2) objetivos de control:

4.1 Requisitos de seguridad de los sistemas de información
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.

Para el cumplimiento del objetivo, el modelo de Seguridad y Privacidad de la Información-MPSI establece los siguientes controles:

14.1.1 Análisis y especificación de requisitos de seguridad de la información Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
14.1.2 Seguridad de servicios de las aplicaciones en redes públicas Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

14.1.3 Protección de transacciones de los servicios de las aplicaciones Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

14.2 Seguridad en los procesos de desarrollo y soporte:
Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
14.2.1 Política de desarrollo seguro Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
14.2.2 Procedimientos de control de cambios en sistemas Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
14.2.4 Restricciones en los cambios a los paquetes de software Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
14.2.5 Principios de construcción de sistemas seguros Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
14.2.6 Ambiente de desarrollo seguro Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
14.2.7 Desarrollo contratado externamente Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
14.2.8 Pruebas de seguridad de sistemas Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
14.2.9 Prueba de aceptación de sistemas Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.

14.3 Datos de prueba Objetivo: Asegurar la protección de los datos usados para pruebas.

14.3.1 Protección de datos de prueba Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.

El manual de políticas de Seguridad de Información establece políticas para la adquisición y mantenimiento de sistemas de información, adicionalmente en el contrato actual de mantenimiento del Sistemas SAIA a pesar que se establece la cláusula de cumplimiento con la Políticas de Seguridad de la Información del CNMH, no se tiene evidencia de la verificación por parte de los supervisores del cumplimiento de dicha obligación. Lo anterior

teniendo en cuenta que por ejemplo no se tiene evidencia de los requisitos de seguridad del sistema, de la verificación de la política de desarrollo seguro, de la verificación de la aplicación de gestión de cambios entre otros. Se recomienda precisar en los contratos de adquisición y mantenimiento de bienes y servicios TIC se establezcan de forma explícita cuales son las que deben cumplir el proveedor y fortalece la supervisión para asegurar el cumplimiento de los mismos.

Se evidencia que la entidad no ha implementado los controles 14.2.8 Pruebas de seguridad de sistemas Control y 14.2.9 Prueba de aceptación de sistemas Control lo cual incrementa la probabilidad de adquirir productos sin el cumplimiento de la calidad técnica requerida. Se recomienda diseñar, implementar y aplicar los controles relacionados con las pruebas de los productos adquiridos con el fin de mitigar el riego de calidad de los productos que pueden impactar la disponibilidad, integridad y confidencialidad de la información que estos gestionan.

de los principios de seguridad exigencia de requisitos de seguridad de las aplicaciones y los mantenimientos contratados. establece explícitamente lo exigido en las políticas para este tipo de servicios

**CONTROLES DOMINIO 15 RELACIÓN CON LOS PROVEEDORES**

Este Dominio establece dos (2) objetivos de control:

15.1 Seguridad de la información en las relaciones con los proveedores
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

15.1.1 Política de seguridad de la información para las relaciones con proveedores Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar. 15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
15.1.3 Cadena de suministro de tecnología de información y comunicación Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

15.2 Gestión de la prestación de servicios con los proveedores
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

15.2.1 Seguimiento y revisión de los servicios de los proveedores Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
15.2.2 Gestión de cambios en los servicios de proveedores Control: Se deberían gestionar los cambios en el

suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

*El documento de Políticas de seguridad de la información establece en su numeral 8.21 las políticas relacionadas con proveedores, adicionalmente en algunos contratos de bienes y servicios TIC, se establece la cláusula de cumplimiento de Políticas de Seguridad del CNMH, sin embargo, no se cuenta con evidencia documental que dicha política se haya socializado con los proveedores y entregado copia de las mismas con el fin de asegurar su cumplimiento. Se recomienda realizar un análisis de riesgo de los contratos y determinar de forma concreta cuales son los controles pertinentes para cada uno y asegurar por parte de los supervisores su cumplimiento.*

**CONTROLES DOMINIO 16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

Este Dominio establece un (1) objetivo de control:

16.1 Gestión de incidentes y mejoras en la seguridad de la información
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

16.1.1 Responsabilidad y procedimientos Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
16.1.2 Reporte de eventos de seguridad de la información Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.3 Reporte de debilidades de seguridad de la información Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
16.1.5 Respuesta a incidentes de seguridad de la información Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
6.1.7 Recolección de evidencia Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que

*El SGSI cuenta con un procedimiento de Gestión de Incidentes de Seguridad, el cual se está actualizando por*

*parte del Grupo TIC, sin embargo, no se tienen evidencias documentales de la aplicación del procedimiento con sus respectivos registros. Se recomienda fortalecer las actividades de seguimiento, monitoreo y documentación propios de la Gestión de incidentes de seguridad las cuales permitan tener un reporte oportuno, la evaluación y análisis del mismo, la determinación de las causas, determinar acciones preventivas o correctivas y contar con evidencia documental para prevenir futuros materializaciones de los incidentes*

**CONTROLES DOMINIO 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**

Este Dominio establece dos (2) objetivos de control:

17.1 Continuidad de seguridad de la información
Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

17.1.1 Planificación de la continuidad de la seguridad de la información Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. 17.1.2 Implementación de la continuidad de la seguridad de la información Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

17.2 Redundancias Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información. Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

*En la vigencia 2013 el CNMH contrato una consultoría para definir el Plan de Continuidad de Negocio de la Entidad, sin embargo, a la fecha no se tiene evidencia de su implementación. Igualmente, no se tiene evidencia de la implementación de los controles de este Dominio. Se recomienda realizar el análisis de riesgos con el fin de determinar el tratamiento de los mismos y determinar la aplicabilidad de los controles establecidos en la normatividad vigente*.

**CONTROLES DOMINIO 18 CUMPLIMIENTO**

Este Dominio establece dos (2) objetivos de control:

18.1 Cumplimiento de requisitos legales y contractuales
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
18.1.2 Derechos de propiedad intelectual Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 18.1.3 Protección de registros Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
18.1.4 Privacidad y protección de datos personales Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
18.1.5 Reglamentación de controles criptográficos Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

*El manual de Políticas de Seguridad de la Información en su numeral 13 establece el marco normativo aplicable a la seguridad de la información el cual fue actualizado el 25 de septiembre de 2019. se recomienda asegurar la ejecución de actividades para su respectiva actualización y aprobación de acuerdo con la dinámica normativa.*

*Adicionalmente se evidencia que el CNMH cuenta con controles procedimentales y automáticos para el control de la propiedad intelectual en materia de software y licencias de uso.*

18.2 Revisiones de seguridad de la información
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

18.2.1 Revisión independiente de la seguridad de la información Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
18.2.2 Cumplimiento con las políticas y normas de seguridad Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

18.2.3 Revisión del cumplimiento técnico Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Se evidencia que el CNMH ha realizado revisiones al SGSI a través del proceso de evaluación control del área de Control Interno durante la vigencia de 2019 y este informe hace parte de la revisión para la vigencia 2020, sin embargo, las revisiones periódicas no están establecidas formalmente como control dentro del proceso de Evaluación y Control.

Adicionalmente el Comité Institucional de Gestión y Desempeño realizó la revisión del SGSI durante la vigencia de 2019, sin embargo, a la fecha no se ha realizado la revisión de la vigencia 2020. Se recomienda programar en la agenda del Comité la Revisión para esta vigencia.

**CONCLUSION**

*El CNMH ha venido implementado el SGSI desde la vigencia 2016, dicho sistema hace parte del Sistema Integrado de Gestión-SGI, no obstante, lo anterior se observan debilidades en la sostenibilidad e implementación de los controles propios del modelo de privacidad y seguridad de la información. Entre las principales causas de dichas debilidades se presenta las siguientes:*

1- *Ausencia de liderazgo y gobernabilidad del SGSI de forma centralizada por parte de la DAYF-Grupo TIC, la cual impacta en la eficiencia y efectividad de las acciones en torno al SGSI. Lo anterior se evidencia en la ausencia de la asignación del Rol del Líder del SGSI con el empoderamiento necesario para el liderazgo y sostenibilidad del Sistema.*
2- *Carencia de indicadores de implementación del SGSI que permitan medir e identificar el estado de avance y desviaciones en la implementación del SGSI.*
3- *Desactualización de la Declaración de Aplicabilidad de Controles del SGSI. Contar con una Declaración de Aplicabilidad revisada, actualizada y aprobada permitirá acotar el alcance del SGSI ante la dinámica de riesgos y estrategia actual de la Entidad.*

*Para la definición del Plan del Mejoramiento se recomienda tener en cuenta las causas relacionadas anteriormente más las identificadas por lo líderes del proceso.*

**MATRIZ PARA PLAN DE MEJORAMIENTO**
**(Metodología para elaboración - fecha de entrega)**

| No | DESCRIPCION DEL HALLAZGO | RECOMENDACION |
|---|---|---|
| 1 | **Controles Dominio 5 Política de Seguridad** | Se recomienda fortalecer las actividades de socialización y capacitación del SGSI a nivel interno y |

| | | |
|---|---|---|
| | Se evidencia que la Política ha sido socializada en lo corrido del 2019 a los servidores públicos del CNMH, sin embargo, no se evidencia que se hayan realizado socializaciones y capacitaciones durante la vigencia del 2020 y tampoco se evidencia su socialización a partes externas como son proveedores o entidades externas que lo requieran.<br><br>En el artículo segundo de la Resolución 206 de 2018 se establece que la Política de Seguridad debe revisarse con periodicidad al menos anual por parte del Comité Institucional de Gestión y Desempeño. En lo corrido de la vigencia 2020 no se han realizado revisiones de la Política de SGSI, se recomienda que se programa dicha revisión en la agenda del Comité.<br><br>De acuerdo con lo establecido en el Artículo Tercero de la Resolución 206 de 2018 y en el Artículo Décimo Cuarto de la Resolución 038 del 31 de enero de 2018, No se evidencia que en los Comités Institucionales de Gestión y Desempeño celebrados durante 2020 se haya presentado por parte del líder de Seguridad de Información del CNMH el estado de avance de la implementación del SGSI, adicionalmente no se evidencia que el Comité haya hecho seguimiento a las acciones para la implementación de los controles del SGSI. Por lo anterior se recomienda que se incluya en la agenda del Comité Institucional de Gestión y Desempeño el seguimiento al estado del SGSI. | externo, en especial a proveedores del CNMH. Lo anterior teniendo en cuenta que en los contratos con proveedores se establece el cumplimiento de las Políticas de Seguridad de la Información por parte de estos en la minuta contractual.<br><br>Se recomienda que se programe en la Agenda del Comité Institucional de Gestión y Desempeño la revisión del SGSI para la vigencia 2020. |
| **2** | **Controles Dominio 6 Organización de la seguridad de la información**<br><br>Se evidencia que en el numeral 6. ESTRUCTURA ORGANIZACIONAL del | Se recomienda se revisé la asignación del Rol de Oficial de Seguridad de Información y se establezcan formalmente la funciones correspondientes, lo anterior con el fin de asegurar la sostenibilidad del SGSI y mitigar los riesgos de disponibilidad, |

| | | |
|---|---|---|
| | documento: SIP-MA-002 Manual Sistema Gestión Seguridad Información, se establecen responsabilidades para la seguridad de la información. Adicionalmente recomienda la creación del Rol de OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.<br><br>Sin embargo, a la fecha no se evidencia que el CNMH haya nombrado y asignado las funciones específicas para el rol de Oficial de Seguridad de la Información de acuerdo con lo definido en el Manual de SGSI. | integridad y confidencialidad de la información. |
| **3** | **Controles Dominio 8 Gestión de Activos**<br><br>El control 8.2.2 Etiquetado de la información Modelo de Seguridad y Privacidad de la Información establece que se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.<br><br>Se evidencia que el CNMH implemento el control mediante el procedimiento SIP-PR-011 V1 Etiquetado_de_Información, sin embargo, no se tiene evidencia que el control se esté aplicando ya que no se evidencio la existencia de los formatos SIP-FT-013 establecidos en dicho procedimiento. | Se recomienda la revisión y aplicación del control establecido en el procedimiento SIP-PR-011-Etiquetado de la información, y dejar evidencia de los registros establecidos en dicho procedimiento. |
| **4** | **Controles Dominio 9. Control de Acceso a la Información**<br>Se evidencia que el CNMH implemento el control mediante el procedimiento SIP-PR-008. Registro y cancelación de cuentas de usuario. V1. Sin embargo, se evidencia que la gestión de acceso a los sistemas de información no se aplica los | Se recomienda estandarizar la política y procedimientos de gestión de acceso para los sistemas de información y los servicios de Red, con el objetivo de tener control centralizado de los usuarios finales y usuarios administradores (súper usuarios). Se recomienda que las claves de acceso de usuario administrador se custodien por métodos |

| | | |
|---|---|---|
| | controles establecidos. La descentralización de la operación del módulo de seguridad de los diferentes sistemas de Información genera debilidad en el control de acceso.<br><br>Se evidencia que los siguientes controles establecidos en este Dominio a la fecha no están implementados:<br>A.9.2.4 Gestión de información de autenticación secreta de usuarios<br>A.9.2.5 Revisión de los derechos de acceso de usuarios<br>A.9.3.1 Uso de la información de autenticación secreta<br>A.9.4.5 Control de acceso a códigos fuente de programas | seguros para asegurar su confidencialidad, integridad y disponibilidad de la información<br><br>Se recomienda verificar que la totalidad de los sistemas de información misionales y de apoyo gestionen las contraseñas para asegurar que sean de calidad y controlen cambio periódico e interactivo de las mismas<br><br>Se recomienda se revise el tratamiento de riesgos de los controles no implementados y se defina el plan de trabajo para su respectiva implementación y aplicación. |
| **5** | **Controles Dominio 12 Seguridad de las operaciones**<br><br>Se evidencia que no se cuenta la bitácora centralizada de cambios de la plataforma tecnológica interna y de los proveedores para la vigencia 2019 y 2020 tanto a nivel de hardware, software operativo y aplicaciones que soportan los sistemas de información, lo anterior muestra debilidades en la gestión de cambios de la plataforma y generando dificultades al momento contar con información para el análisis de incidentes de seguridad de la información. Lo anterior se materializo con el incidente de seguridad del sistema de gestión documental.<br><br>Se evidencia que el CNMH cuenta con equipos para efectuar copias de respaldo al igual que para los servicios contratados externamente se tiene contratado el servicio de copias de respaldo. Sin embargo, se evidencia que no se realizan las pruebas a las copias de respaldo con | Se recomienda fortalecer los controle de gestión de cambios con el fin de contar con una traza de los cambios realizados en la plataforma tecnológica propia y aplicarla a los proveedores previo del análisis de riesgo pertinente.<br><br>Se recomienda fortalecer el control de copias de respaldo definiendo la política de pruebas de las copias de respaldo y hacerla extensiva a los contratos con los proveedores correspondientes.<br><br>se recomienda se defina diseñe, implemente y se apliquen los controles pendientes: 12.4.1 Registro de eventos Control, 12.4.2 Protección de la información de registro Control, 12.4.3 Registros del administrador y del operador Control<br>Se recomienda diseñar, implementar y aplicar controles para realizar el análisis de vulnerabilidad de la plataforma tecnológica del CNMH con carácter prioritario. |

| | | |
|---|---|---|
| | el fin de asegurar su consistencia y disponibilidad. Se recomienda fortalecer el control de copias de respaldo definiendo la política de pruebas de dichas copias y hacerla extensiva a los contratos con los proveedores correspondientes<br><br>Se evidencia que no se cuenta con la implementación de los controles 12.4.1 Registro de eventos Control, 12.4.2 Protección de la información de registro Control, 12.4.3 Registros del administrador y del operador Control. se recomienda se defina diseñe, implemente y se apliquen los controles pendientes. Adicionalmente se evidencio que el sistema de gestión documental no cuenta con traza de auditoria que permita identificar las actividades del administrador lo cual genera riesgos de integridad, disponibilidad y confidencialidad de la información.<br><br>Se evidencia que el control 12.6.1 Gestión de las vulnerabilidades técnicas y por lo tanto no se cuenta con información de las vulnerabilidades de la plataforma tecnológica y como consecuencia no se cuenta con actividades para mitigar dichas vulnerabilidades. | |
| **6** | **Controles Dominio 13 Seguridad de las Comunicaciones**<br>Se evidencia que no cuenta con la documentación formal del grupo de controles del objetivo 13.2 Transferencia de Información, sin embargo, existen controles automáticos como el FireWall que permite filtrar el tráfico para cada servidor, la mensajería electrónica se gestiona de forma segura a través de filtros implementados en el firewall el cual mitiga el | Se recomienda formalizar y documentar las políticas correspondientes y demás documentos necesarios para asegurar la sostenibilidad de los controles. |

| | | |
|---|---|---|
| | riesgo de integridad de la información, adicionalmente se cuenta con software antivirus el cual protege la mensajería electrónica al interior de la Red LAN. | |
| **7** | **Controles Dominio 14 Aadquisición, Desarrollo y Mantenimientos de sistemas**<br><br>El manual de políticas de Seguridad de Información establece políticas para la adquisición y mantenimiento de sistemas de información, adicionalmente en el contrato actual de mantenimiento del Sistemas SAIA a pesar que se establece la cláusula de cumplimiento con la Políticas de Seguridad de la Información del CNMH, no se tiene evidencia de la verificación por parte de los supervisores del cumplimiento de dicha obligación. Lo anterior teniendo en cuenta que por ejemplo no se tiene evidencia de los requisitos de seguridad del sistema, de la verificación de la política de desarrollo seguro, de la verificación de la aplicación de gestión de cambios entre otros.<br><br>Se evidencia que la entidad no ha implementado los controles 14.2.8 Pruebas de seguridad de sistemas Control y 14.2.9 Prueba de aceptación de sistemas Control lo cual incrementa la probabilidad de adquirir productos sin el cumplimiento de la calidad técnica requerida. | Se recomienda precisar en los contratos de adquisición y mantenimiento de bienes y servicios TIC se establezcan de forma explícita cuales políticas de seguridad son las que debe cumplir el proveedor y fortalecer la supervisión para asegurar el cumplimiento de los mismos.<br><br>Se recomienda diseñar, implementar y aplicar los controles relacionados con las pruebas de los productos adquiridos con el fin de mitigar el riegos de calidad de los productos que pueden impactar la disponibilidad, integridad y confidencialidad de la información que estos gestionan |
| **8** | **Controles Dominio 15 Relación con los Proveedores** | Se recomienda realizar un análisis de riesgo de los contratos y determinar de forma concreta cuales son los controles pertinentes para cada proveedor y asegurar por parte de los supervisores su |

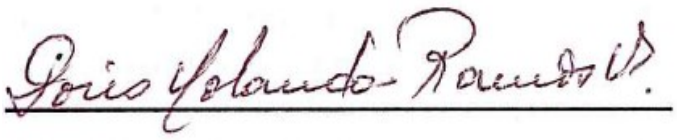
| | | |
|---|---|---|
| | El documento de Políticas de seguridad de la información establece en su numeral 8.21 las políticas relacionadas con proveedores, adicionalmente en algunos contratos de bienes y servicios TIC se establece la cláusula de cumplimiento de Políticas de Seguridad del CNMH, sin embargo, no se cuenta con evidencia documental que dicha política se haya socializado con los proveedores y entregado copia de las mismas con el fin de asegurar su cumplimiento. | cumplimiento. |
| **9** | **Controles Dominio 17 Gestión de la Continuidad del Negocio.**<br><br>En la vigencia 2013 el CNMH contrato una consultoría para definir el Plan de Continuidad de Negocio de la Entidad, sin embargo, a la fecha no se tiene evidencia de su implementación. Igualmente, no se tiene evidencia de la implementación de los controles de este Dominio. | Se recomienda realizar el análisis de riesgos con el fin de determinar el tratamiento de los mismos y determinar la aplicabilidad de los controles establecidos en la normatividad vigente. |
| **10** | **Controles Dominio 18 Cumplimiento**<br><br>El SGSI cuenta con un procedimiento de Gestión de Incidentes de Seguridad el cual se está actualizando por parte del Grupo TIC, sin embargo, no se tienen evidencias documentales de la aplicación del procedimiento con sus respectivos registros. | Se recomienda fortalecer las actividades de seguimiento, monitoreo y documentación propios de la Gestión de incidentes de seguridad las cuales permitan tener un reporte oportuno, la evaluación y análisis del mismo, la determinación de las causas, determinar acciones preventivas o correctivas y contar con evidencia documental para prevenir futuros materializaciones de los incidentes. Adicionalmente se recomienda que la actualización del procedimiento involucre de forma precisa cada uno de los controles establecido en el Dominio 16 del Modelo de Seguridad y Privacidad de la Información. |
| **11** | Se evidencia que el CNMH ha realizado revisiones al SGSI a través del proceso de evaluación control del área de Control Interno durante la vigencia de 2019 y este informe hace | Se recomienda formalizar el control de revisiones independientes del SGSI de forma periódica en el proceso de Evaluación y Control, lo anterior de acuerdo con lo establecido en el Modelo de |

| | | |
|---|---|---|
| | parte de la revisión para la vigencia 2020, sin embargo, las revisiones periódicas no están establecidas formalmente como control dentro del proceso de Evaluación y Control.<br><br>Adicionalmente el Comité Institucional de Gestión y Desempeño realizo la revisión del SGSI durante la vigencia de 2019, sin embargo, a la fecha no se ha realizado la revisión de la vigencia 2020. | Seguridad y Privacidad de la Información en su control 18.2.1 Revisión independiente de la seguridad de la información<br><br>Se recomienda programar en la agenda del Comité la Revisión para la vigencia 2020. |

## OPORTUNIDADES DE MEJORA

**1.** Los conjuntos de controles en el Dominio Seguridad Física y del Entorno se encuentran establecidos en el documento de Políticas de Seguridad de la información, sin embargo, se recomienda actualizar los pertinentes teniendo en cuenta las nuevas condiciones de operación del CNMH motivadas por la emergencia sanitaria. Lo anterior teniendo en cuenta por ejemplo que algunos funcionarios se les ha entregado equipos de cómputo para trabajo remoto.

## FIRMAS RESPONSABLES

| **Auditor** | **Vo. Bo.** |
|---|---|
|  <br>José Edgar Hernando Galarza Bogotá - Contratista |  <br>Doris Yolanda Ramos Vega – Asesora de Control Interno |