AUDITORÍA / EVALUACIÓN Y SEGUIMIENTO : Implementación controles Sistema de Seguridad de Información – SGSI en la Dirección de Archivo de Derechos Humanos

LUGAR: Bogotá D,C. CNMH Calle 34 #5-27

FECHA: 30/05/2019

AUDITOR: José Edgar Hernando Galarza Bogotá

I OBJETIVO GENERAL.

Seguimiento al estado de avance de la implementación de controles del Sistemas de Gestión de Seguridad – SGSI el cual es requisito de la normatividad vigencia en el marco de la Política de Gobierno Digital y hace parte del Plan de Mejora del hallazgo 45 del plan de Mejoramiento subscrito con la Contraloría General de la República – CGR.

II OBJETIVOS ESPECÍFICOS.

- Verificar el estado de avance de la implementación de los controles del Sistema de Seguridad de la Información-SGSI basado en el Modelo de Seguridad y Privacidad de la Información y/o ISO-27000-2013 en la Dirección de Archivo de Derechos Humanos.

III 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.

IV ALCANCE.

Verificación del estado de avance de la implementación de Controles del Sistema de Gestión de Seguridad de Información en la Dirección de Archivo de Derechos Humanos. El seguimiento tendrá cobertura para los controles identificados con los numerales: 5. Política de Seguridad, 6. Organización de la Seguridad de la Información, 7. Seguridad de los Recursos Humanos, 8. Gestión de Activos, 9. Control de Acceso a la Información, 10. Criptografía, 11. Seguridad Física, 12. Seguridad de las Operaciones del Modelo de Seguridad y Privacidad de la Información.

V 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, entrevistas, revisión de la información disponible en el Sistema Integrado de Gestión y la dispuesta por el líder del proceso y el Análisis de la información enviada por el Grupo TIC y la Dirección de Archivo de Derechos Humanos. El seguimiento fue realizado entre el 3 de marzo y el 15 de mayo de 2019.

VI LIMITACIONES.

Los requerimientos de información solicitados al grupo TIC se recibieron de forma parcial fuera de los términos de tiempo establecidos, por lo anterior se hizo necesario dividir el alcance del seguimiento en dos fases. A continuación se describe la bitácora del requerimiento de información.

1. La solicitud de información se realizó el 18 de marzo de 2019 con un alcance de información sobre el 100% de los controles definidos en el MSPI y se estableció el termino de entrega para el 26 de marzo

2. El grupo TIC manifestó no poder cumplir con la fecha establecida y se concedió de común acuerdo como fecha de entrega el 11 de abril de 2019.
3. El término de tiempo establecido en el punto anterior no se pudo cumplir por parte del grupo TIC y DADH, finalmente se recibe información parcial el 2 de mayo de 2019, con un avance de entrega del 18%.
4. En vista de lo anterior y con el fin de dinamizar el seguimiento, control interno propuso al grupo TIC realizar la entrega de la información en dos fases.
   - La primer fase con alcance del 42% de los controles y fecha de entrega el 13 de mayo
   - La segunda fase con alcance del restante 58% de los controles y fecha de entrega el 30 de agosto. Lo anterior se formalizo mediante comunicación electrónica de Control Interno del 7 de mayo.
5. La entrega de la información de la primera se realizó el 20 de mayo, sin embargo se recibe nuevamente parcialmente la información.
6. Teniendo en cuenta el cronograma del Programa Anual de Auditoria, el cual fue aprobado por el Comité Coordinador de Control Interno, este informe se elabora con base en la información referenciada en el numeral 5. Por lo anterior el alcance de este informe cubre los dominios: 5. Política de Seguridad, 6. Organización de la Seguridad de la Información, 7. Seguridad de los Recursos Humanos, 8. Gestión de Activos, 9. Control de Acceso a la Información y dejara fuera del alcance los Dominios: 10. Criptografía, 11. Seguridad Física, 12. Seguridad de las Operaciones lo cuales se revisarán en la segunda fase.

VII NORMATIVIDAD.

- Decreto 1008 de Junio 2018 del MINTIC, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- Resolución 206 de 2018 del Centro Nacional de Memoria Histórica por medio del cual se adopta la Política de Seguridad de Información.
- Sistema de Gestión de Seguridad de la Información que hace parte del Sistema Integrado de Gestión del CNMH
- Modelo de Seguridad y Privacidad de la Información del MINTIC
- ISO 27001:2013. Anexo A.

VIII DESARROLLO DE LA AUDITORÍA.

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 para los controles, su implementación formal y la aplicación que ha tenido en la Dirección de Archivo de Derechos Humanos.

A continuación se muestra para cada control, la descripción del mismo de acuerdo con el Modelo de Seguridad y Privacidad de la Información-MSPI del MINTIC, las características de la implementación en el CNMH y la aplicación en la Dirección de Archivo de Derechos Humanos

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. Adicionalmente mediante la Resolución Interna 206 de 23 de julio de 2018 se adoptó dicha Política.

Se evidencia que la Política ha sido socializada en lo corrido del 2019 a los servidores públicos de la Dirección de Archivo de Derechos Humanos - DADH mediante sesiones de capacitación. Sin embargo no se evidencia que se hayan realizado socializaciones o capacitaciones durante la vigencia del 2018

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.

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 el 2018 y lo corrido del 2019 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.

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.

De acuerdo con La Resolución Interna 206 de 23 de julio de 2018, la resolución 038 de 31 de enero de 2018 y la Resolución 233 de septiembre de 2018 que deroga la 038 de 2018, mediante las cuales se establecen las funciones del comité Institucional de Gestión y desempeño no se evidencia que el Comité (2018,2019) 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.

EL grupo TIC informa que en este control no se implementa "teniendo en cuenta que la entidad no tiene deberes ni áreas de responsabilidad que puedan generar conflicto." Es importante dejar registro de la justificación de en la Declaración de aplicabilidad.

6.1.3 Contacto con las autoridades: Se deberían mantener los contactos apropiados con las autoridades pertinentes.

Se evidencia que el control no se ha implementado formalmente a la fecha, sin embargo el grupo TIC informa "Se tiene conciencia de que hay que tener contacto con las autoridades, pero no se evidencia procedimiento formal. Se cuenta con un listado de autoridades: CSIRT, colCERT, Cai Virtual. El CNMH se encuentra suscrito en el CSIRT de la Policía Nacional."

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 funcionario 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 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 aseguré 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 implementó el control mediante la política SIP-PC-010 V1 Política de teletrabajo, aprobada y publicada en la intranet el 05/08/2016, sin embargo no se evidencia que se esté aplicando ya que no se tiene evidencia física o electrónica de las Autorizaciones para realizar teletrabajo.

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 comprendan sus responsabilidades y son idóneos 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 acuerdo de confidencialidad para todos los funcionarios del área, y que aplica a todos los funcionarios del Centro y contratistas Este último formato a la fecha no está formalizado en el Sistema de Gestión de Seguridad de Información*.

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. *Adicionalmente para la vigencia del 2019 el Grupo TIC cuenta con un contrato de prestación de servicios profesionales para apoyar la gestión del SGSI.*

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 durante la vigencia de 2019 el Grupo TIC viene ejecutando un plan de socialización del SGSI.

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.

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 mis 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 con un inventario de activos revisado y aprobado cuya última fecha de actualización fue el 1 de diciembre de 2017, adicionalmente el SGSI cuenta una metodología de clasificación de Activos y un procedimiento de clasificación de activos-SIP-PR-016. Sin embargo se observa que la metodología y el procedimiento, no se han aplicado durante el 2018. En el mes de mayo de 2019 la Dirección Administrativa y Financiera solicito a todas las áreas del CNMH iniciar el proceso de actualización del inventario de Activos de Información.

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

Se evidencia que el CNHM en el inventario de activos de información de la DADH contiene la relación de los activos de información y sus propietarios, la fecha de última actualización de inventario de activos se realizó el 1 de diciembre de 2017.

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 implemento 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 reciba 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 CNMH cuenta cuentan con una metodología de clasificación de Activos y un procedimiento de clasificación de activos-SIP-PR-016. Sin embargo se observa que la metodología y el procedimiento no se han aplicado durante el 2018 y lo corrido del 2019 en la Dirección de Archivo de Derechos Humanos.

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 implemento 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 evidencia 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". Sin embargo no se tiene evidencia de la aplicación de la Metodología de Clasificación de Activos en la Dirección de Archivo de Derechos Humanos durante el periodo de evaluación.

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 en el CNMH no se 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 v1.

En la aplicación del protocolo, se observa que la documentación del intercambio de información se realiza mediante Acta, sin embargo dicha Acta no es un documento estructurado que permita de manera eficiente verificar los prerrequisitos establecidos en el numeral 4 y las consideraciones del numeral 6. Por lo anterior se presenta el riesgo de intercambio de información sin el cumplimiento de los prerrequisitos establecidos.

No se evidenció la existencia del documento de autorización del dueño o custodio de la información a las personas que participan del intercambio de la información, lo anterior de acuerdo con lo establecido en el numeral 5 del protocolo de intercambio de información.

Se evidenció que en la Dirección de Archivo de Derechos Humanos se intercambió información utilizando discos externos, lo anterior no cumple con los medios establecidos en el numeral 4.1 Prerrequisitos que establece "Que el canal de comunicaciones sea seguro (VPN, protocolos cifrados, correo electrónico, correo certificado, transporte a través de vehículo blindado, integración o interfaces entre aplicativos).

CONTROLES DOMINIO 9. CONTROL DE ACCESO A LA INFORMACIÓN

Este Dominio establece tres (3) objetivos de control, de los cuales se evaluarán dos dentro del alcance de este informe, teniendo en cuenta la disponibilidad de la información entregada por los auditados.

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, sin embargo no se evidencia dentro del SIG que esta política esté desarrollada y documentada.

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 no se evidencia la aplicación en la DADH del procedimiento y tampoco se utiliza el formato de Novedad de cuentas de Usuario. SIP-FT-021.

Actualmente la DADH gestiona la autorización retiro o asignación de acceso a los servicios de red de sus funcionarios mediante comunicación por correo electrónico al grupo TIC, sin aplicar el procedimiento establecido correspondiente.

Se evidencia que la operación del módulo de usuarios del Sistema de Información del Archivo de Derechos Humanos no se realiza por el área de TIC, como lo hace con otras aplicaciones como es el caso del módulo de seguridad del sistema de Información Humano. La descentralización de la operación del módulo de seguridad de los diferentes sistemas de Información genera debilidad en el control de acceso.

Para terminar los objetivos de control y sus controles correspondientes para los dominios 10. Criptografía, 11. Seguridad Física y 12. Seguridad de Operaciones no se revisaron teniendo en cuenta lo anotado en el numeral VI LIMITACIONES de este informe. Dichos controles se revisarán en un segundo seguimiento que se realizará en el segundo semestre de acuerdo con el Cronograma del Plan Anual de Auditoria.

IX OPORTUNIDADES DE MEJORAMIENTO.

PLAN DE MEJORAMIENTO:

A continuación se relacionan las acciones que deben llevarse a PLAN DE MEJORAMIENTO. Para el efecto los responsables de las acciones deben realizar el diligenciamiento del FORMATO CIT-PR-002 Plan de mejoramiento V2 el cual se encuentra en la Intranet en el Sistema Integrado de Gestión, dentro del proceso de Control Interno. Según el procedimiento interno CIT-PR-002 V2 se debe remitir el FORMATO debidamente diligenciado dentro de los ocho (8) días contados a partir de la recepción del informe de auditoría.

N	O/H	DESCRIPCIÓN	RECOMENDACIÓN
1	O	Se evidenció que la Política de Seguridad de Información ha sido socializada en el mes de marzo del 2019 a los servidores públicos de la Dirección de Archivo de Derechos Humanos - DADH mediante sesiones de capacitación. Sin embargo no se evidencia que se hayan realizado socializaciones o capacitaciones durante la vigencia del 2018. Lo anterior es una de las causas del desconocimiento del SGSI y sus respectivos controles al igual de las responsabilidades que se deben asumir.	Definir un plan de uso y apropiación que permita de manera eficiente que el SGSI sea apropiado y aplicado por los servidores públicos de acuerdo con sus funciones y/o obligaciones.
2	H	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 el 2018 y lo corrido del 2019 se haya presentado por parte del líder de Seguridad de Información del CNMH el estado de avance de la implementación del SGSI,	Se recomienda que el Comité Institucional de Gestión y Desempeño incluya en su agenda en lo posible de forma permanente el seguimiento y orientación para el cumplimiento de la Política de Gobierno Digital de la cual la Seguridad Digital es un elemento habilitador de la misma. Lo anterior de acuerdo con la normatividad vigente que establece el Rol de dicho Comité.

		adicionalmente no se evidencia que el Comité haya hecho seguimiento a las acciones para la implementación de los controles del SGSI.	
3	H	Se evidenció que el CNMH implemento el control mediante la política SIP-PC-010 V1 Política de teletrabajo, aprobada y publicada en la intranet el 05/08/2016, sin embargo no se evidenció que se esté aplicando ya que no se tiene evidencia física o electrónica de las Autorizaciones para realizar teletrabajo.	Se recomienda revisar las condiciones de los funcionarios de grupos regionales en el marco de la política de Teletrabajo y aplicar el control correspondiente.
4	O	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. EL grupo TIC informa que el control 6.1.2 Separación de deberes: no se implementa "teniendo en cuenta que la entidad no tiene deberes ni áreas de responsabilidad que puedan generar conflicto." No se evidencia que la justificación se haya formalizado en la declaración de aplicabilidad del SGSI.	Se recomienda que para los controles que el CNMH haya decidido no implementar se deje justificación documentada en la declaracion de aplicabilidad del sistema de seguridad de información-SGSI
5	H	De acuerdo con el MSPI el control Se evidencia que los controles ***6.1.3 Contacto con las autoridades,***	Se recomienda que los controles se definan, documenten, formalicen y se implementen en el marco del SGSI

		6.1.4 Contacto con grupos de interés especial, ***6.1.5 Seguridad de la información en la gestión de proyectos*** NO se han implementado formalmente en el SGSI. Sin embargo cabe anotar que el Grupo TIC ha adelantado actividades informales relacionadas con estos controles	
6	O	De acuerdo con el MSPI, el control ***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 evidenció que el CNHM cuenta cuentan con un inventario de activos revisado y aprobado por la Dirección cuya última fecha de actualización fue el 1 de diciembre de 2017, adicionalmente el SGSI cuenta una metodología de clasificación de Activos y un procedimiento de clasificación de activos-SIP-PR-016. Sin embargo se observa que la metodología y el procedimiento no se han aplicado durante el 2018. En el mes de mayo de 2019 la Dirección Administrativa y Financiera solicito a todas las áreas del CNMH iniciar el proceso de actualización del inventario de Activos de Información.	Se recomienda fortalecer los mecanismos de seguimiento y monitoreo del SGSI con el fin de asegurar la actualización periódica de los activos de información del CNMH

7	O	De acuerdo con el MSPI, el control ***8.1.2 Propiedad de los activos: Los activos mantenidos en el inventario deberían tener un propietario.*** Se evidenció 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 actualización de inventario de activos se realizó el 1 de diciembre de 2017. Durante la vigencia 2018 no se evidencia actualización del inventario de activos.	Se recomienda fortalecer las campañas de socialización y capacitación del SGSI así como también el liderazgo de los diferentes responsables del SGSI para asegurar el cumplimiento de las responsabilidades de los diferentes actores ante la implementación, sostenibilidad y mejoramiento del SGSI
8	H	De acuerdo con el MSPI, el control ***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 evidenció que el CNHM cuenta cuentan con una metodología de clasificación de Activos y un procedimiento de clasificación de activos-SIP-PR-016. Sin embargo se observa que la metodología y el procedimiento no se han aplicado durante el 2018 y lo corrido del 2019 en la Dirección de Archivo de Derechos Humanos.	Se recomienda fortalecer los mecanismos de seguimiento y monitoreo del SGSI con el fin de asegurar la aplicación de los controles establecidos en el SGSI
9	H	De acuerdo con el MSPI, el control	Se recomienda fortalecer los mecanismos de seguimiento y monitoreo del SGSI con el fin de

		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 evidenció que el CNMH implemento 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.	asegurar la aplicación de los controles establecidos en el SGSI
10	H	De acuerdo con el MSPI, el control ***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 evidenció que el CNMH implemento 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	Se recomienda fortalecer los mecanismos de seguimiento y monitoreo del SGSI con el fin de asegurar la aplicación de los controles establecidos en el SGSI

		actividad 9-Resgistro de Gestión de dicho procedimiento.	
11	H	De acuerdo con el MSPI, el control ***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 evidenció que el CNMH no se ha implementado formalmente este control en el SGSI.	Se recomienda que los controles se definan, documenten, formalicen y se implementen en el marco del SGSI
12	H	De acuerdo con el MSPI, el control ***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 evidenció que el CNMH implemento el control mediante el procedimiento SIP-PT-001 Protocolo de intercambio seguro de información v1. En la aplicación del protocolo se observa que la documentación del intercambio de información se realiza mediante Acta, sin embargo dicha Acta no es un documento estructurado que permita de manera eficiente verificar los prerrequisitos establecidos en el numeral 4 y las consideraciones del numeral 6. Por lo anterior se presenta el riesgo de intercambio	Se recomienda que las actividades de intercambio de información se realizan aplicando estrictamente lo establecido en los procedimientos del SGSI. En caso de requerir realizar actividades diferentes a las establecidas es necesario la actualización y formalización del mismo de forma oportuna ante los administradores del Sistema Integrado de Gestión.

		de información sin el cumplimiento de los prerrequisitos establecidos. No se evidenció la existencia del documento de autorización del dueño o custodio de la información a las personas que participan del intercambio de la información, lo anterior de acuerdo con lo establecido en el numeral 5 del protocolo de intercambio de información. Se evidenció que en la Dirección de Archivo de Derechos Humanos se intercambió información utilizando discos externos, lo anterior no cumple con los medios establecidos en el numeral 4.1 Prerrequisitos que establece "Que el canal de comunicaciones sea seguro (VPN, protocolos cifrados, correo electrónico, correo certificado, transporte a través de vehículo blindado, integración o interfaces entre aplicativos).	
13	H	De acuerdo con el MSPI, los 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***	Se recomienda fortalecer los mecanismos de seguimiento y monitoreo del SGSI con el fin de asegurar la aplicación de los controles establecidos en el SGSI. Se recomienda centralizar la operación de los módulos de seguridad y/o gestión de usuarios de los diferentes sistemas de información sea centralizada en el Grupo TIC o el Rol de Oficial de Seguridad de la Información.

		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 evidenció que el CNMH implemento el control mediante el procedimiento SIP-PR-008. Registro y cancelación de cuentas de usuario. V1. Sin embargo no se evidencia la aplicación en la DADH del procedimiento y tampoco se utiliza el formato de Novedad de cuentas de Usuario. SIP-FT-021. Actualmente la DADH gestiona la autorización retiro o asignación de acceso a los servicios de red de sus funcionarios mediante comunicación por correo electrónico al grupo TIC, sin aplicar el procedimiento establecido correspondiente.	

		Se evidenció que la operación del módulo de usuarios del Sistema de Información del Archivo de Derechos Humanos no se realiza por el área de TIC, como lo hace con otras aplicaciones como es el caso del módulo de seguridad del sistema de Información Humano. La descentralización de la operación del módulo de seguridad de los diferentes sistemas de Información genera debilidad en el control de acceso.	

X CONCLUSIÓN.

El CNMH ha implementado el SGSI durante la vigencia 2016, dicho sistema hace parte integral del Sistema Integrado de Gestión, no obstante lo anterior se observan debilidades en la aplicación de los controles implementados por causa principalmente por desconocimiento de los mismos por parte de las áreas responsables. Igualmente se observa que la Administración del CNMH no ha definido y asignado el rol de Oficial de Seguridad de Información lo cual genera debilidades en la implementación, el liderazgo, el monitoreo y mejoramiento del SGSI.

XI FIRMAS RESPONSABLES

Auditor:	Vo. Bo.
José Edgar Hernando Galarza Bogotá Contratista Control Interno - Auditor	Doris Yolanda Ramos Vega - Asesora de Control Interno