Fecha emisión del informe	día	22	mes	07	año	2025

Proceso:	Gestión de Tecnología de la Información y las Comunicaciones
Procedimiento/operaciones.	Matriz de Riesgos de Seguridad Digital.
Líder de Proceso: Jefe(s) Dependencia(s):	Líder del proceso de apoyo.
Nombre del seguimiento:	Seguimiento de Control Interno (tercera línea) a Mapa de Riesgos de Seguridad de la Información.
Objetivo:	Realizar seguimiento al mapa de riesgos de seguridad de la información y evaluar la efectividad de los controles definidos.
Metodología	El seguimiento se realizó conforme al análisis de la información solicitada por Control Interno y entregada por la Dirección Administrativa y Financiera DAyF – TIC mediante correo electrónico del 10 de junio de 2025. Adicionalmente se realizaron consultas en el sistema integrado de gestión de la entidad.
Limitaciones o riesgos del proceso de seguimiento	No se presentaron limitaciones en el desarrollo de este informe.

Asesor de Control Interno	**Equipo Evaluador de Control Interno**
Doris Yolanda Ramos Vega	Willson Ernesto Albarracin Gómez

DESARROLLO DEL SEGUIMIENTO

Introducción y Normatividad

La administración del riesgo y diseño de controles en las entidades públicas se fundamenta, en general, en el criterio metodológico establecido en la *"Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas versión 6"* expedida por el Departamento Administrativo de la Función Pública – DAFP. En lo que respecta específicamente al objeto del presente seguimiento (los riesgos asociados a la seguridad de la información), dicho enfoque se complementa con los lineamientos establecidos en algunas normas y disposiciones técnicas como la:

- Norma ISO/IEC 27001:2022 *"Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, Sistemas de gestión de la Seguridad de la Información".*
- Norma ISO/IEC 27005:2024 *"Gestión de Riesgos de Seguridad de la Información"*.
- Resolución Nro. 02277 de junio 3 de 2025, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), junto con su anexo técnico *"Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, versión 2025"*.

Adicionalmente, el presente seguimiento se desarrolla con base en el **Rol Evaluación de la Gestión del Riesgo**, descrito en la *"Guía Rol de la Unidades u Oficinas de Control Interno, Auditoría Interna o quien Haga sus Veces versión 3 (septiembre de 2023)".* Este rol tiene como propósito proporcionar un aseguramiento técnico y objetivo a la Alta Dirección (línea estratégica)

respecto al diseño y efectividad de las actividades de administración del riesgo, a fin de garantizar que los riesgos clave o estratégicos, estén debidamente identificados, gestionados de forma apropiada y alineados con la operación institucional, por el impacto que representan en la operación y eficacia del sistema de control interno.

Definiciones.

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27001:2022).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001:2022).
- **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001:2022).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. El control es también utilizado como sinónimo de salvaguarda o contramedida; en una definición más simple, es una medida que modifica el riesgo (MSPI).
- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27001:2022).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implementar los controles necesarios para proteger la misma. (ISO/IEC 27000) (MSPI).
- **Gestión de incidentes de seguridad de la información:** Procesos o actividades desarrolladas para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27001:2022).
- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite, o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022) (MSPI).
- **Modelo de Gobernanza de Seguridad digital:** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos

e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país. (Decreto 338-2022) (MSPI).

CONSIDERACIÓN INICIAL

Antes de iniciar y presentar los resultados de este seguimiento es importante mencionar que dentro de las evidencias aportadas por la Dirección Administrativa y Financiera - Gestión de TIC (DAyF-Gestión de TIC), se encuentra el documento "*Informe seguimiento al mapa de riesgos*", al corte 30 de junio de 2025, el cual es de gran importancia porque incluye un diagnóstico sobre el estado de la matriz de riesgos y la gestión institucional del riesgo de seguridad de la información, en donde en resumen se pueden señalar aspectos importantes como:

En la sección "*Estado actual*" se indica que el CNMH cuenta con una matriz de riesgos de seguridad de la información; sin embargo, esta no refleja adecuadamente los riesgos tecnológicos actuales ni las transformaciones recientes en la gestión de servicios e infraestructura. Aunque existen controles implementados, no están debidamente documentados en la matriz, lo que limita su utilidad como herramienta de monitoreo y toma de decisiones. Esta situación evidencia la necesidad urgente de actualizar y alinear la matriz con el Decreto 620 de 2020, la Ley 1581 de 2012 y los lineamientos del SGSI bajo estándares internacionales.

De otra parte, en el "*Estado Deseado*" del documento se plantea la necesidad de reformular integralmente la matriz de riesgos de seguridad de la información del CNMH, alineándola con la norma ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI). Esta nueva versión debe incorporar controles actualizados, evidencias verificables, responsables definidos y mecanismos de evaluación periódica. Además, debe integrarse con el SGSI y el sistema de gestión documental institucional, garantizando su trazabilidad y auditabilidad. Esta actualización permitirá anticipar riesgos, priorizar acciones preventivas y fortalecer la resiliencia del CNMH frente a incidentes de seguridad.

Informe del plan de acción para la actualización de la matriz de riesgos

Adicionalmente la DAyF - Gestión de TIC, remitió el informe titulado "*Plan de Acción para la Actualización de la Matriz de Riesgos de Seguridad de la Información*", el cual constituye un ejercicio técnico valioso, ya que no se limita a cumplir con una obligación formal, sino que propone una reformulación integral de la matriz, articulando diagnóstico, normativa aplicable, estado deseado, riesgos por inacción y un plan de acción concreto.

El informe parte de una premisa clave expresada por el mismo equipo responsable: la protección de la información es un eje transversal para garantizar la confidencialidad, integridad y disponibilidad de los activos críticos del CNMH, en especial por el carácter sensible e histórico de los datos que administra la entidad. A partir de esta visión, se reconoce que la matriz vigente, aunque contiene controles activos, no refleja adecuadamente el contexto tecnológico actual ni permite una trazabilidad efectiva de las acciones implementadas.

En este sentido, el diagnóstico presentado por Gestión TIC sobre la matriz de riesgos, junto con el plan de acción formulado, representan un paso importante hacia una gestión de riesgos más madura, basada en evidencia y alineada con estándares internacionales como la ISO/IEC 27001:2022, la ISO/IEC 27005 y el Modelo de Seguridad y Privacidad de la Información (MSPI), así como con la Ley 1581 de 2012, el Decreto 620 de 2020 y los lineamientos del MIPG.

No obstante, pese a la gestión demostrada por la DAyF - Gestión de TIC y al plan de acción allegado, el presente seguimiento se desarrolla teniendo en cuenta las evidencias presentadas y el estado actual del mapa de riesgos de seguridad de la información, con el fin de brindar un instrumento para la toma de decisiones, en aras de la mejora continua y el fortalecimiento de la gestión del riesgo.

RESULTADOS

1. Seguimiento al mapa de riesgos de seguridad de la información.

La gestión del riesgo y su evaluación debe considerar la planificación institucional, los marcos normativos vigentes y la protección de los activos de información estratégicos. El CNMH ha dispuesto un mapa de riesgos de seguridad digital, el cual fue publicado en el Sistema Integrado de Gestión el 30 de mayo de 2025 y constituye el insumo evaluado para este ejercicio técnico. En dicho documento Control Interno identifica un solo riesgo asociado a dos (2) activos de información diferentes y con descripción distinta, junto con sus propiedades o atributos y siete (7) controles definidos para su tratamiento, así:

Tabla 1. Riesgos de seguridad digital CNMH 2025

Activo	Riesgo	Descripción del Riesgo	Controles
Servidor de datos DELL (Dirección administrativa y financiera - Gestión de TIC Transversal a todos los procesos del CNMH)	Pérdida de la Integridad, disponibilidad y confidencialidad de la información.	Deficiencia en las condiciones físicas y ambientales del centro de datos, las fluctuaciones de energía y la necesidad de controles adecuados para el acceso al mismo, propician las condiciones que pueden generar daños en el servidor DELL y como consecuencia pérdida de la integridad, disponibilidad y confidencialidad de la información contenida en él.	4
Infraestructura de servidores y almacenamiento contratada en nube privada	Pérdida de la Integridad, disponibilidad y confidencialidad de la información.	Deficiencia en la contratación de los recursos de procesamiento, almacenamiento y seguridad en nube privada, así como del canal de comunicación entre el CNMH y el proveedor de los servicios, propician las condiciones que pueden generar pérdida de información, vulnerabilidades de seguridad y como consecuencia pérdida de la integridad, disponibilidad y confidencialidad de la información.	3

Fuente: MapaRiesgosSegDigital_2024.

Una vez evaluado el contenido del documento en Excel "MapaRiesgosSegDigital_2024", se evidencia un trabajo de identificación, descripción, clasificación y valoración del riesgo; sin embargo, es necesario realizar un análisis ampliado y más detallado de los puntos de riesgo sobre los objetivos estratégicos, los procesos, los procedimientos, las áreas de impacto y los factores de riesgo, en concordancia con lo definido en la *"Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas",* para tener mayor cobertura en la protección de la información y lograr la plena identificación de los riesgos que puedan afectar el cumplimiento de los objetivos del CNMH.

Un ejemplo de lo anterior se evidencia en el procedimiento denominado "Respaldo y Recuperación de la Información" (código GTC-PR-007, versión 2), el cual, a pesar de estar formalmente documentado, no presenta ningún riesgo ni control asociado en el mapa de riesgos de seguridad de la información. Esta omisión podría comprometer el cumplimiento de su objetivo, que es "*garantizar la integridad y disponibilidad de los datos o sistemas de información alojados en los diferentes servidores y/o repositorios de información ubicados en el centro de cómputo del CNMH, determinando su administración y control de las copias de respaldo que sean generadas a partir del software seleccionado para tal fin*". La ausencia de una identificación clara de los riesgos inherentes a este procedimiento, así como la falta de controles definidos para su mitigación, limita su capacidad de protección ante eventos como la pérdida de información y la indisponibilidad de datos requeridos para asegurar la continuidad operativa de los procesos institucionales.

De otro lado, no es conveniente asociar en una sola línea de riesgo los tres criterios de Confidencialidad, Integridad y Disponibilidad, ya que cada dimensión puede tener causas, impactos y controles distintos.

Por ejemplo, para el riesgo con la descripción "*Deficiencia en las condiciones físicas y ambientales del centro de datos, las fluctuaciones de energía y la necesidad de controles adecuados para el acceso al mismo, propician las condiciones que pueden generar daños en el servidor DELL y como consecuencia pérdida de la integridad, disponibilidad y confidencialidad de la información contenida en él*", *se entiende que las variaciones de energía afectan principalmente la disponibilidad, el acceso físico no controlado compromete la confidencialidad y el daño físico al servidor puede alterar la integridad de la información, por lo que la agrupación realizada en el mapa dificulta la priorización y diseño de controles específicos, lo que puede debilitar la correcta gestión de este riesgo*.

De igual modo frente al riesgo con la descripción "*Deficiencia en la contratación de los recursos de procesamiento, almacenamiento y seguridad en nube privada, así como del canal de comunicación entre el CNMH y el proveedor de los servicios, propician las condiciones que pueden generar pérdida de información, vulnerabilidades de seguridad y como consecuencia pérdida de la integridad, disponibilidad y confidencialidad de la información*", se evidencia que incluye más de un posible riesgo, cuya gestión sería diferente para cada uno.

Así por ejemplo, frente a la pérdida de disponibilidad de la información la causa puede estar asociada a fallas en la contratación o garantía del canal de comunicación y el control propuesto puede ser la realización de pruebas de continuidad o redundancia del canal, mientras que frente a la pérdida de integridad de la información, la causa puede estar asociada al procesamiento inadecuado o errores del proveedor, sobre lo cual podrían definirse controles como validaciones

automáticas, checksum o registros de integridad. Como puede evidenciarse se está hablando de riesgos diferentes, con los cuales podrían identificarse causas y controles independientes, pero que en la matriz se encuentran unificados, dificultando una correcta gestión y tratamiento de los riesgos.

Considerando lo expuesto, se recomienda desde Control Interno individualizar el riesgo registrado en el mapa, teniendo en cuenta que las descripciones no son las mismas, fortalecer el proceso de identificación de los riesgos de seguridad de la información y realizar la desagregación de cada riesgo en líneas independientes por criterio afectado, lo cual mejora la trazabilidad y el diseño y asignación de los controles que sean necesarios.

Ahora bien, frente a la matriz de riesgo suministrada y en relación con el Riesgo Residual, se evidencia una calificación "Débil" para tres (3) controles frente a criterios como ejecución, solidez individual y solidez conjunta que ameritan la ejecución de un Plan de Acción para el fortalecimiento del *control, que según el mapa se observa que la Fecha de Finalización de Implementación es 2019-09-24. Además, hay un (1) control denominado "El Profesional Especializado de la Dirección Administrativa y Financiera Gestión de TIC, anualmente verificará que las licencias tanto del firewall como del antivirus estén activas y en sus últimas versiones con el objetivo de contar con los medios de prevención ante ataques informáticos, instrucciones y virus. Como evidencias se contará con los contratos suscritos. En caso de no contar con estos medios el tráfico cursado en la red será completamente vulnerable", que no cuenta con la evaluación de la ejecución y, por último, se encuentran tres (3) controles con una evaluación de solidez individual y conjunta en nivel moderado.*

Teniendo en cuenta lo anterior, se recomienda revisar y actualizar de manera integral todo el mapa y además garantizar el correcto diligenciamiento y funcionamiento del Excel, para avanzar hacia una gestión más madura, proactiva y efectiva de la seguridad de la información institucional.

2. Madurez del proceso de gestión del riesgo de Seguridad de la Información

Para realizar la evaluación del nivel de madurez del proceso de gestión del riesgo de Seguridad de la Información en el CNMH, se tomaron como referencia las cinco etapas progresivas de madurez: *Inicial, Repetible, Definido, Administrado y Optimizado*, conforme a lo definido en la "*Guía rol de las Unidades u Oficinas de Control Interno, Auditoría Interna o quien haga sus veces*".

Bajo este enfoque, Control Interno diseñó conforme a la guía los siguientes criterios específicos de valoración para cada una de estas etapas, con base en referentes técnicos y normativos vigentes en materia de gestión del riesgo, a fin de generar una evaluación objetiva, contextualizada y alineada con los principios y lineamientos institucionales sobre gestión del riesgo:

Tabla 2. Criterios de evaluación del nivel de madurez del proceso

Etapas de madurez	Descripción del nivel de madurez	Criterios de evaluación propuestos para el proceso de gestión de riesgos de seguridad de la información
Inicial	La gestión del riesgo es reactiva y no sistemática. No existe un marco definido. Las acciones se toman solo ante incidentes ocurridos.	I1: No existe una matriz de riesgos de seguridad de la información formal. I2: No hay responsables asignados ni evidencia documental. I3: No se han definido políticas o procedimientos. I4: No se realizan actividades periódicas de evaluación. I5: No existe una terminología compartida. I6: No se han definido niveles de apetito o tolerancia al riesgo. I7: No se utiliza la información de riesgos para la toma de decisiones ni la planeación.
Repetible	Se han identificado algunos riesgos, pero de manera parcial y sin metodología clara. Las acciones son esporádicas y no se documentan de forma consistente.	R1: Existe una matriz básica o preliminar de riesgos de seguridad de la información. R2: Hay prácticas repetidas frente a los riesgos sin formalización ni retroalimentación. R3: No se evidencia un ciclo sistemático de identificación, valoración y tratamiento. R4: Se manejan algunos conceptos básicos de riesgos, sin estandarización. R5: Se hacen juicios subjetivos sobre la aceptación del riesgo. R6: Se aplican criterios de evaluación del riesgo de manera aislada o sin rigurosidad. R7: El uso de la información de la gestión de riesgos es ocasional, sin trazabilidad.
Definido	El proceso está formalizado en políticas y procedimientos. Se aplica con regularidad. Hay responsables definidos y herramientas básicas para seguimiento.	D1: Existe un procedimiento y política documentada y aprobada con el compromiso de la alta dirección, en donde se establezcan los criterios para la gestión del riesgo. D2: El mapa (matriz) de riesgos de seguridad de la información está publicada. D3: Se han identificado responsables y roles para la gestión del riesgo. D4: Se evidencia la aplicación periódica de las etapas del ciclo de riesgo (identificación, análisis, valoración, tratamiento, seguimiento y comunicación). D5: Existe un lenguaje técnico definido y utilizado por las áreas responsables del riesgo. D6: Existen registros documentados que evidencian decisiones sobre aceptación, transferencia o mitigación de riesgos. D7: La entidad cuenta con los recursos (por ejemplo, económicos, talento humano) para la gestión del riesgo. D8: El uso de la información de riesgos es utilizada para la formulación de planes y controles.
Administrado	La gestión del riesgo es integral, proactiva y se monitorea. Se toman decisiones basadas en los análisis. Hay seguimiento a controles y acciones correctivas.	A1: Se tienen documentados todos los procesos y procedimientos necesarios para garantizar la integridad, disponibilidad y confidencialidad de la información. A2: Se tienen identificados y valorados todos los posibles riesgos asociados con amenazas que puedan comprometer el adecuado manejo, protección, recuperación y valor de los activos de información. A3: Se tienen definidos e implementados los controles de seguridad de la información conforme a la ISO/IEC 27001:2022.

		A4: Se realizan análisis causa-raíz para cada uno de los riesgos, sus causas y se actualiza la matriz periódicamente. A5: Los conceptos asociados a riesgos son comprendidos y usados transversalmente, y hacen parte de la cultura organizacional. A6: La evaluación de riesgos se integra al ciclo de gestión institucional. A7: Se utiliza la información de la gestión de riesgos para la toma decisiones y ajustes operativos de manera permanente.
Optimizado	La gestión del riesgo está integrada a la estrategia institucional. Se mejora de forma continua y se utilizan herramientas tecnológicas para su gestión.	O1: Uso de métricas de desempeño y alertas tempranas. O2: Retroalimentación constante con base en datos, auditorías y resultados. O3: Automatización de reportes y análisis. O4: Alineación con objetivos institucionales y estrategia TI. O5: El lenguaje del riesgo está institucionalizado y es parte de la cultura organizacional. O6: La aceptación del riesgo se revisa periódicamente en función de cambios estratégicos. O7: La evaluación del riesgo está automatizada, es predictiva y está orientada a decisiones. O8: La información de la gestión de los riesgos se vincula directamente con la planeación, inversión y gestión del desempeño.

Fuente: Elaboración propia considerando referentes como la Guía para la Administración del Riesgo, Guía rol de las unidades u oficinas de Control Interno, Auditoría Interna o quien haga sus veces, Norma ISO/IEC 27005:2022 y el Modelo Integrado de Planeación y Gestión (MIPG).

Una vez definidos los criterios por etapa, estos se compararon frente a tres dimensiones clave del proceso, de acuerdo con la *"Guía Rol de las Unidades u oficinas de Control Interno, Auditoría Interna o quien haga sus veces",* las cuales se resumen a continuación:

- **Gobierno**, hace referencia al liderazgo, la asignación de responsabilidades y la articulación con la alta dirección y los entes de control.
- **Cultura**, entendida como el grado de apropiación, concienciación y compromiso frente al riesgo en los distintos niveles de la entidad.
- **Procesos**, centrados en la existencia, aplicación y seguimiento del procedimiento institucional para la identificación, análisis y tratamiento de los riesgos de seguridad de la información.

Así las cosas, analizada la información suministrada por la DAyF - Gestión de TIC, a continuación, se muestra el resultado obtenido de cruzar los criterios de cada etapa entre las dimensiones, lo cual permite identificar brechas, fortalezas y oportunidades de mejora de manera estructurada, para facilitar la formulación de acciones orientadas al fortalecimiento continuo del proceso de gestión del riesgo en la entidad:

Tabla 3. Evaluación por Dimensiones

Dimensión Cultura	Dimensión Gobierno	Dimensión Proceso
• El mapa de riesgos muestra avances en el uso de un lenguaje técnico por parte de Gestión de TIC (D5). • La DAyF - Gestión de TIC ha impulsado actividades para revisar y actualizar técnicamente los activos de información y el mapa de riesgos (D4).	• Existen el procedimiento Administración del Riesgo SIP-PR-007 Versión 6 del 19 de enero de 2024, aprobado e incorporado en el Sistema Integrado de Gestión de la Entidad (D1). • La alta dirección del CNMH está comprometida con la gestión del riesgo y expide la Resolución 378 del 26 de diciembre de 2023 "Por medio de la cual actualiza la política de administración del riesgo en el Centro Nacional de Memoria Histórica" (D1). • Existen roles y responsables definidos dentro del procedimiento y el mapa de riesgos (D3) • Se observa asignación de recursos para la gestión de riesgos de seguridad de la información, por ejemplo, a través de la contratación de servicios en la nube y servicios de conexión del enlace dedicado de conectividad terrestre a internet. (D7).	• El mapa de riesgos incluye elementos técnicos claves como aceptación del riesgo, impacto, probabilidad, controles, riesgo residual, entre otros (D6). • En el Sistema Integrado de Gestión se observa el mapa de riesgos institucional de fecha 30 de mayo de 2025. Este mapa incluye los riesgos de seguridad de la información (D2). • El informe de seguimiento y el informe de acciones de mejora elaborados por la DAyF - Gestión de TIC, muestran que se están consolidando los procedimientos institucionales para fortalecer el proceso, estandarizar los formatos, corregir los errores técnicos y promover un uso más sistemático y confiable de la matriz (D8).

Fuente: Elaboración propia

Teniendo en cuenta los resultados presentados en la Tabla 3, se concluye que el proceso de gestión del riesgo de seguridad de la información del CNMH se encuentra en la etapa de madurez **"Definido"**, al evidenciarse avances en las tres dimensiones evaluadas conforme a los criterios diseñados de Cultura, Gobierno y Proceso. En cuanto a la dimensión de Cultura, se observa que el mapa de riesgos incorpora un lenguaje técnico relacionado con la seguridad de la información, y que Gestión de TIC ha promovido actividades orientadas a la revisión y actualización de los activos de información.

Desde la perspectiva de Gobierno, se destaca la existencia del procedimiento de Administración del Riesgo aprobado e incorporado en el Sistema Integrado de Gestión - SIG, así como el compromiso de la alta dirección del CNMH, reflejado en la aprobación de la actualización de la política. De igual forma, tanto en el procedimiento como en el mapa se hace referencia a roles y responsables y desde la ordenación del gasto, se evidencia la asignación de recursos para apoyar la gestión del riesgo.

En la dimensión de Procesos, se resalta que el mapa de riesgos incluye elementos técnicos clave, como la metodología para el análisis y evaluación del riesgo inherente y residual, la definición de controles y responsables; también Gestión de TIC ha elaborado documentos como el informe de seguimiento al mapa de riesgos y el informe de acciones de mejora a la matriz, los cuales evidencian que el proceso se encuentra en ejecución y cuenta con elementos de seguimiento.

Para que el proceso de gestión del riesgo de seguridad de la información en el CNMH avance desde la fase "Definido" hasta la fase "Administrado", es primordial afianzar por completo lo ya establecido en el nivel presente. *Esto supone por ejemplo que, los componentes estructurados existentes como son la política, el procedimiento, el mapa de riesgos y la asignación de roles, no solo estén documentados, sino que sean aplicados de manera constante, revisados periódicamente y se gestionen de forma dinámica en toda la entidad; igualmente, se requiere definir y ejecutar indicadores de desempeño que son fundamentales para la gestión del riesgo porque permiten medir, controlar y mejorar el proceso de forma objetiva porque "lo que no se mide, no se puede gestionar ni mejorar". Solo cuando estos elementos estén completamente integrados y operando de manera continua, podrá considerarse que el proceso ha alcanzado un mayor grado de madurez.*

En este contexto, a continuación, se presentan algunas recomendaciones para afianzar el proceso en esta etapa:

- Fortalecer el proceso de identificación de los riesgos de seguridad de la información, garantizando su alineación con los activos de información institucional, los procesos críticos y las amenazas tecnológicas actuales. Una identificación adecuada constituye la base para una evaluación, tratamiento y monitoreo efectivos, y permite garantizar la pertinencia de los controles y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

- Realizar una revisión y ajuste integral del mapa de riesgos de seguridad de la información, con el fin de completar los campos vacíos, corregir errores o fórmulas incorrectas (por ejemplo, registros con el valor '#N/D'), mejorar la trazabilidad entre los riesgos identificados y los controles implementados y actualizar el plan de acción para el fortalecimiento de los controles. Estas acciones son necesarias para garantizar la calidad, consistencia y confiabilidad de la información registrada, y así asegurar que la matriz cumpla su función como herramienta efectiva para el análisis, monitoreo y toma de decisiones sobre los riesgos institucionales.

- ***Implementar, en concordancia con los riesgos identificados, nuevos controles y fortalecer los que ya existen, con el fin de proteger la información institucional a través de acciones, como, por ejemplo, mejorar la seguridad de acceso a los sistemas, realizar copias de seguridad de los archivos importantes, detectar posibles accesos no autorizados, reforzar la seguridad de los sistemas que manejan datos sensibles, entre otros***.

- Definir y establecer indicadores de desempeño específicos para la gestión del riesgo de seguridad de la información, que faciliten el monitoreo continuo del proceso, la evaluación de la eficacia de los controles implementados y la toma de decisiones basadas en evidencia por parte de la alta dirección.

- ***Realizar en el marco del Comité Institucional de Gestión y Desempeño presentaciones con los resultados de las evaluaciones periódicas sobre el uso efectivo de la matriz de riesgos de seguridad de la información, con el fin de promover decisiones informadas relacionadas con la aceptación de riesgos***.

- Implementar herramientas que respalden la gestión integral de los riesgos de seguridad de la información, priorizando soluciones que permitan automatizar funciones clave como el monitoreo continuo de la infraestructura tecnológica, la detección y gestión de vulnerabilidades, el registro y análisis de incidentes de seguridad, y el seguimiento al cumplimiento de controles y planes de tratamiento. Estas herramientas deben facilitar la trazabilidad, la generación de alertas tempranas y la toma de decisiones basadas en datos reales.

- Actualizar el "*Plan de Tratamiento de Riesgos*" con código SIP-PL-003, versión 1, emitido el 30 de noviembre de 2017, en concordancia con los lineamientos establecidos en la Guía de Administración del Riesgo del DAFP (versión 6 de 2022), el Modelo de Seguridad y Privacidad de la Información (MSPI versión 4 de 2025) y las normas internacionales ISO/IEC 27001:2022 e ISO/IEC 27005:2022, con el propósito de definir las acciones necesarias para reducir, controlar o manejar el riesgo actual y los nuevos que se identifiquen, asignando responsables, recursos y plazos, en aras de proteger los activos institucionales y tomar decisiones informadas para garantizar la confidencialidad, integridad y disponibilidad de la información.

- Continuar con el plan de acción para la actualización de la matriz de riesgos liderado por la Dirección Administrativa y Financiera – Gestión TIC, asegurando los entregables propuestos y su alineación con la normatividad vigente en la materia.

- Promover actividades periódicas de sensibilización institucional orientadas a la apropiación, concientización y compromiso frente a la gestión del riesgo por parte de los funcionarios en los distintos niveles de la entidad incluyendo, por ejemplo, temas relacionados con amenazas o vectores de ataque comunes (phishing, malware, ingeniería social, ransomware, fugas de información, acceso a sitios web maliciosos, entre otros), en concordancia con lo definido en el numeral 9 de las "*Políticas de seguridad y privacidad de la información", versión 004.*

- Incorporar en el Sistema Integrado de Gestión los procedimientos mencionados en las "*Políticas de seguridad y privacidad de la información", versión 004.*

3. Valoración de la efectividad de los controles

Este apartado presenta la evaluación de efectividad de los controles definidos en la matriz de riesgos de seguridad de la información del CNMH. Para cada control se analizaron los atributos clave como claridad, diseño, aplicación, frecuencia, responsable y evidencia, complementándolos con la valoración de su naturaleza (manual, automática o híbrida), el tipo de control (preventivo, detectivo o correctivo) y su grado de alineación con la causa del riesgo. Para este ejercicio se tuvo en cuenta la documentación técnica y administrativa suministrada por el área DAyF-TI, incluyendo informes de mantenimiento, evidencia contractual, reportes técnicos y el mapa de riesgos institucional.

Como resultado, se emitió un juicio técnico de efectividad que clasifica los controles en los siguientes niveles:

- **Alta**: El control está bien diseñado, debidamente implementado, alineado con la causa del riesgo y genera evidencia suficiente de su eficacia para mitigar razonablemente la amenaza.
- **Moderada**: El control cumple parcialmente con los atributos evaluados; si bien contribuye a la mitigación del riesgo, presenta limitaciones en su alineación, diseño, aplicación o cobertura que afectan su efectividad general.
- **Baja**: El control es insuficiente, inadecuado o ineficaz frente al riesgo identificado; presenta deficiencias significativas en su diseño, aplicación o trazabilidad, o no guarda alineación directa con la causa del riesgo o lo hace de manera parcial.

Esta valoración permite identificar oportunidades de mejora, fortalecer el esquema de control del CNMH y apoyar la toma de decisiones orientadas a una gestión más robusta de la seguridad de la información.

A continuación, se presenta la verificación de cada control con base en la evidencia recibida y analizada:

Evaluación efectividad control No 1:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Servidor de datos DELL – Gestión de TIC (transversal a todos los procesos del CNMH)	
Causa del riesgo	Falta de control de la temperatura en el cuarto de datos.
Control definido	El Profesional Especializado de la Dirección Administrativa y Financiera - Gestión de TIC, semestralmente incorporará al informe de mantenimiento del segundo y cuarto trimestre la información sobre el estado del centro de datos referente a sus condiciones físicas y ambientales, con el propósito de generar las acciones preventivas o de mejora en caso de presentarse cambios que puedan representar un aumento del riesgo de daños sobre los equipos. De no ser así se pueden presentar daños en el servidor por deterioro en las condiciones ambientales al interior del cuarto de datos.
Tipo de control	Preventivo. Permite identificar condiciones físicas y ambientales que pueden derivar en la materialización del riesgo, posibilitando la adopción de acciones correctivas antes de que se presenten fallas en la infraestructura tecnológica.
Naturaleza	Manual (depende de la elaboración de un informe por parte del profesional especializado).
Alineación con la causa	Parcial. Aunque el control contribuye a identificar condiciones ambientales desfavorables en el centro de datos, su enfoque es reportar la situación en cortes semestrales, lo cual no representa un control directo ni continuo sobre la variable de temperatura. Por tanto, si bien guarda relación con la causa del riesgo, no la mitiga plenamente al no existir una periodicidad adecuada.
Evaluación de atributos del control	
Claridad	El control está definido en cuanto a su objetivo, periodicidad (semestral) y responsable (Profesional Especializado de Gestión TIC).
Diseño	Adecuado, pero con baja frecuencia y dependencia de reporte humano, lo cual limita su efectividad preventiva. El control está estructurado como parte del proceso formal de mantenimiento preventivo de servidores y centros de datos, integrando acciones físicas (limpieza, revisión, etiquetado, ventilación, revisión eléctrica) y acciones lógicas (respaldos, escaneo antivirus, actualizaciones de sistema operativo). Está enfocado a mitigar riesgos de disponibilidad, continuidad y fallas ambientales, específicamente por temperatura inadecuada o condiciones adversas en el cuarto de datos.
Aplicación	Se evidencia la ejecución del control en junio de 2025, documentada en un informe técnico, con

	cronograma, bitácoras y registros fotográficos.
Frecuencia	Aunque la frecuencia semestral cumple con lo definido en el control, puede ser insuficiente para condiciones ambientales que cambian con mayor rapidez, como la temperatura, lo que deja ventanas de vulnerabilidad en amplios períodos de tiempo intermedios.
Responsable	El control tiene un responsable claramente designado (Profesional Especializado de Gestión de TIC), con participación activa de ingenieros y tecnólogos, y validación de la Dirección Administrativa y Financiera.
Evidencia	Informe de "Mantenimiento Preventivo (Físico y Lógico) de los Servidores y Almacenamientos del CNMH" de junio 2025, que incluye soporte técnico y registros operativos: bitácora de ingreso, cronograma, correos de autorización, registros de temperatura, respaldo fotográfico, respaldos de servidores, menciones a fallas de UPS y aire acondicionado.
Nivel de efectividad	Moderada. El control cumple con los criterios de diseño, aplicación y documentación. Se evidencian en el informe de mantenimiento acciones preventivas y correctivas concretas (respaldo, limpieza, verificación de aire acondicionado, redundancia eléctrica), lo cual mitiga razonablemente el riesgo de daño a los servidores por condiciones físicas desfavorables. Aunque el informe incorpora información sobre las condiciones físicas y ambientales del centro de datos, el control no menciona una medición sistemática continua de temperatura ni la integración de sensores de monitoreo automático con alertas. La frecuencia semestral puede no ser suficiente si ocurren variaciones abruptas en el ambiente del data center.

Con base en la evaluación realizada, el Control No. 1 presenta un nivel de efectividad **moderada**, al permitir la verificación de las condiciones físicas y ambientales del centro de datos, contribuyendo así a mitigar parcialmente el riesgo de pérdida de la integridad, disponibilidad y confidencialidad de la información. El control cuenta con evidencia documental y es ejecutado conforme a lo programado; sin embargo, su aplicación semestral y su carácter principalmente informativo limitan su capacidad para intervenir de forma directa y oportuna la causa del riesgo. Por tanto, se considera que existe una alineación parcial entre la causa y el control, lo cual sugiere la necesidad de complementarlo con mecanismos de monitoreo más frecuentes y de ser posible automatizados, para mejorar la capacidad de acción ante variaciones críticas en el ambiente.

Evaluación efectividad control No 2:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Servidor de datos DELL – Gestión de TIC (transversal a todos los procesos del CNMH)	
Causa del riesgo	Fluctuaciones de energía.
Control definido	El profesional Especializado de la Dirección Administrativa y Financiera - Gestión de TIC, semestralmente contacta al encargado del mantenimiento del edificio torre norte del CC San Martín con el fin de informarse del estado general del sistema de alimentación y respaldo de energía, en caso de presentarse situaciones de posible falla, informará al Director Administrativo y Financiero así como al personal del equipo de trabajo de Gestión de TIC con el fin de asegurar la información contenida en el servidor . De no ser así, la normalización de los servicios se torna más demorada y más dificultosa. Como evidencia, la información del estado del sistema de alimentación de energía se consignará en el informe de mantenimiento del segundo y cuarto trimestre.
Tipo de control	Preventivo. Busca anticiparse a posibles fallas en el sistema eléctrico mediante la verificación del estado del sistema de respaldo, y permite tomar medidas para proteger los activos de información antes de que ocurra un incidente. Se podrían detectar señales tempranas de posibles fallas a través del reporte del encargado del edificio.
Naturaleza	Manual e indirecta (depende de la acción del Profesional Especializado para contactar al encargado del edificio, recopilar la información y documentarla en el informe. El control no menciona el uso de sensores ni sistemas automatizados de verificación o alerta.
Alineación con la causa	Parcial. Aunque el control se relaciona con la causa (fluctuaciones de energía), no actúa directamente sobre ella, ya que el sistema de alimentación depende de la administración del

	edificio. Además, el control es de tipo verificación se recopila información, pero no se interviene ni se realiza monitoreo técnico en tiempo real.
Evaluación de atributos del control	
Claridad	El control tiene definido un propósito, periodicidad, responsables y acciones esperadas.
Diseño	Aunque el control contempla una interacción con el encargado del mantenimiento del edificio para identificar riesgos energéticos, su diseño depende de una gestión de la información (consulta y reporte verbal o por correo), sin instrumentos estandarizados de evaluación ni protocolos de verificación técnica directa.
Aplicación	En el informe de mantenimiento de junio de 2025 se evidencia que hubo contacto con la administración del edificio, registros de ingreso, revisión de UPS, mantenimientos eléctricos y observaciones documentadas sobre fallas (ej. UPS en modo bypass).
Frecuencia	Se aplica semestralmente conforme al control, pero las condiciones eléctricas pueden variar con mayor frecuencia. La reactividad del control depende del reporte de terceros.
Responsable	Está claramente asignado al Profesional Especializado de Gestión de TIC, con reporte al Director Administrativo y Financiero.
Evidencia	El Informe de "Mantenimiento Preventivo (Físico y Lógico) de los Servidores y Almacenamientos del CNMH" de junio 2025 que documenta temas relacionados con la infraestructura eléctrica.
Nivel de efectividad	Moderada. El control se ejecuta conforme a lo establecido y cuenta con evidencia de su aplicación. Permite anticiparse a posibles interrupciones del suministro eléctrico a través del contacto con la administración del edificio y la identificación de fallas en el sistema de respaldo (UPS). Además, se documenta en el informe semestral de mantenimiento. Esto contribuye a reducir parcialmente el riesgo de afectación a la integridad y disponibilidad de la información contenida en el servidor institucional; sin embargo, el control tiene una naturaleza manual y dependiente de terceros, lo cual lo hace vulnerable a errores de comunicación, omisiones o falta de oportunidad en la información recibida. Su frecuencia semestral es limitada frente a la variabilidad de las condiciones eléctricas, y no incorpora mecanismos de monitoreo en tiempo real ni verificación técnica independiente. Además, no actúa directamente sobre la causa del riesgo, lo que afecta su alineación y efectividad estructural.

El Control No. 2 presenta un nivel de efectividad **moderada**, al permitir identificar potenciales fallas en el sistema de respaldo de energía mediante el contacto periódico con la administración del edificio. Su aplicación se verificó en el informe de mantenimiento de junio de 2025, donde se evidencian acciones asociadas y seguimiento a fallas persistentes como la UPS en bypass. No obstante, la alineación con la causa del riesgo es parcial, dado que el control no actúa directamente sobre la infraestructura eléctrica ni establece mecanismos de monitoreo autónomos o continuos. Además, su diseño depende de terceros y no se evidencia la formalización técnica o protocolos específicos de respuesta ante fluctuaciones que garanticen una respuesta adecuada frente a la posible pérdida o daño de los datos institucionales. Se recomienda integrar este control con planes de respaldo y recuperación de datos para garantizar la disponibilidad del servidor y la integridad de la información.

Evaluación efectividad control No 3:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Servidor de datos DELL – Gestión de TIC (transversal a todos los procesos del CNMH)	
Causa del riesgo	Deficiencia en sistemas de control de acceso al centro de datos.
Control definido	El profesional Especializado de la Dirección Administrativa y Financiera - TIC, diariamente realiza visita al cuarto de datos con el objetivo de revisar las condiciones generales y de acceso, así mismo controla la llave de acceso y permite sólo accesos a personal autorizado por la Dirección Administrativa y Financiera y en caso de que personal ajeno al Gestión de TIC requiera acceso, este debe ser autorizado y contar con el acompañamiento del Profesional Especializado de Gestión de TIC o quien Este designe. Como evidencia se cuenta con los registros escritos en la bitácora del cuarto de datos.

Tipo de control	Preventivo. Tiene el objeto de evitar el acceso no autorizado al centro de datos mediante control físico directo, con validación de autorizaciones y acompañamiento obligatorio. Actúa antes de que ocurra una afectación al activo de información.
Naturaleza	Manual. Su ejecución depende enteramente de acciones humanas: supervisión diaria, custodia de llave, validación verbal o escrita de autorizaciones y registro en bitácora física. No se apoya en sistemas automatizados de control de acceso, cámaras o alertas.
Alineación con la causa	El control actúa directamente sobre la fuente del riesgo de manera manual, reduciendo de forma efectiva la probabilidad de accesos indebidos.
Evaluación de atributos del control	
Claridad	El control establece la frecuencia, el responsable, el objeto (control de acceso físico) y el procedimiento en caso de requerimientos de ingreso de personal externo.
Diseño	Funcional, aunque se basa exclusivamente en mecanismos manuales (llave física, bitácora, validación verbal), no contempla elementos tecnológicos o automatizados (cerraduras electrónicas, biometría, control con tarjetas, CCTV), lo que limita la robustez del control ante fallas humanos, pérdida de registros o suplantación.
Aplicación	Según el "Informe acceso a Datacenter", se evidencia la ejecución del control mediante registros diarios, observaciones sobre el estado de ingreso, control de llaves y acompañamiento efectivo al personal externo autorizado.
Frecuencia	Es un control diario, lo cual refuerza su efectividad como barrera preventiva constante.
Responsable	Está asignado al Profesional Especializado de Gestión de TIC, con posibilidad de delegación, y se documenta conforme a lo requerido.
Evidencia	El documento "Informe acceso a Datacenter" de junio de 2025 entregado, contiene registros de ingreso, observaciones sobre comportamiento del personal, trazabilidad de accesos y validación del cumplimiento del procedimiento.
Nivel de efectividad	Alta. El control está bien estructurado, es claro en su aplicación, tiene cobertura diaria y actúa directamente sobre la causa del riesgo. La evidencia demuestra cumplimiento sostenido y documentación adecuada de los accesos, lo que permite mitigar de forma significativa la probabilidad de incidentes por acceso no autorizado al centro de datos. La naturaleza manual del control puede implicar riesgo de errores humanos, omisiones, falsificación de registros o pérdida de trazabilidad y adicionalmente no se cuenta con medidas de respaldo automatizadas (por ejemplo, lectores de huella, video vigilancia, alertas de apertura de puertas), lo cual limita la capacidad de supervisión en caso de eventos no controlados o fuera del horario habitual.

El análisis realizado al Control No. 3 presenta un resultado de evaluación en un nivel de efectividad alta, dado que actúa directamente sobre la causa del riesgo relacionada con el acceso no autorizado al centro de datos. La ejecución diaria del control, la claridad en la asignación de responsabilidades y la evidencia documentada en la bitácora de ingreso demuestran que se implementa de manera constante y sostenida. Este mecanismo contribuye significativamente a reducir la probabilidad de afectaciones a la integridad, disponibilidad y confidencialidad de la información alojada en el servidor institucional. No obstante, al tratarse de un control de naturaleza manual, su efectividad depende en gran medida de un ejercicio manual, lo cual representa una vulnerabilidad residual. Por ello, si bien el control es funcional y está correctamente implementado, se recomienda implementar auditorías cruzadas del registro de accesos, validando coherencia entre bitácoras físicas, autorizaciones formales y presencia del personal en sitio, y evaluar la posibilidad de su fortalecimiento mediante herramientas tecnológicas complementarias que refuercen la trazabilidad y minimicen los riesgos de omisión o suplantación.

Evaluación efectividad control No 4:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Servidor de datos DELL – Gestión de TIC (transversal a todos los procesos del CNMH)	
Causa del riesgo	Ataques informáticos, intrusiones y virus.

Control definido	El Profesional Especializado de Gestión de TIC verificará anualmente que las licencias del firewall y del antivirus estén activas y actualizadas, con el fin de asegurar la prevención ante amenazas informáticas. La evidencia se respalda con los contratos vigentes.
Tipo de control	Preventivo. Pretende evitar la materialización de amenazas cibernéticas mediante la validación del licenciamiento de herramientas tecnológicas de protección perimetral (firewall) y de protección contra código malicioso (antivirus).
Naturaleza	Manual con componentes técnicos. Aunque se apoya en tecnologías (firewall, antivirus), el control es ejecutado manualmente a través de la verificación documental de licencias y versiones, sin mecanismos automatizados de alertas, escaneo continuo o monitoreo proactivo desde una consola centralizada.
Alineación con la causa	El control se enfoca en el requisito formal de licenciamiento, lo cual es necesario, pero no suficiente para prevenir ataques informáticos. No incluye la verificación del funcionamiento efectivo de los mecanismos de protección (reglas del firewall, alertas de intrusión, análisis de tráfico o actualizaciones automáticas del antivirus). Por tanto, aborda la causa solo de manera parcial.
Evaluación de atributos del control	
Claridad	El control especifica el objeto (licenciamiento y actualización), responsable (Profesional Especializado TIC), frecuencia (anual) y medios de verificación (contratos).
Diseño	El diseño es adecuado para garantizar la vigencia de licencias, pero no contempla validación técnica del estado funcional y operativo de las herramientas ni la evaluación del entorno de amenazas, ni monitoreo continuo, alertas automatizadas o auditorías de tráfico. Además, la frecuencia anual es insuficiente frente a la dinámica de evolución de amenazas informáticas.
Aplicación	En los informes de "Estado de Licenciamiento Firewall" e "Informe Estado TIGO UNE", ambos de junio de 2025, se evidencia la revisión del estado del firewall, la identificación de riesgos por licencias próximas a expirar y un diagnóstico detallado sobre vulnerabilidades detectadas, lo que demuestra la ejecución del control.
Frecuencia	La verificación anual es limitada frente al ritmo de cambios en el entorno de ciberseguridad, actualizaciones de firmas de virus, aparición de nuevas vulnerabilidades y ciclos de expiración de licencias.
Responsable	Se encuentra asignado al Profesional Especializado de Gestión de TIC, quien también participa en la revisión técnica del estado de conectividad y dispositivos.
Evidencia	Se cuenta con informes que documentan la revisión del licenciamiento, diagnóstico de seguridad, trazabilidad de tickets con el proveedor y estado de dispositivos de red.
Nivel de efectividad	Moderada. El control permite garantizar que los componentes esenciales de protección informática cuenten con licencias vigentes, lo cual representa una condición habilitante para su operación. El control se ejecutó y documentó; sin embargo, la frecuencia anual es insuficiente para un entorno de amenazas altamente dinámico, y no se asegura que las herramientas funcionen correctamente ni que las configuraciones sean óptimas para contener intrusiones. Se evidencia dependencia del proveedor externo TIGO UNE sin mecanismos de control interno complementarios. Por tanto, si bien contribuye parcialmente a mitigar el riesgo, no es una barrera suficientemente robusta por sí sola.

Frente al Control No. 4 se evidencia un nivel de efectividad moderado, dado que se centra en la verificación del licenciamiento activo y actualizado del firewall y el antivirus institucional, lo cual constituye una condición básica para la prevención de ataques informáticos. La evidencia documental demuestra que el control fue ejecutado durante el primer semestre de 2025, mediante diagnósticos técnicos y seguimiento al proveedor. No obstante, la frecuencia anual resulta insuficiente frente al dinamismo y volatilidad del entorno de amenazas, y el control no contempla una validación funcional o técnica continua del estado operativo de estas herramientas. Por tanto, aunque contribuye parcialmente a mitigar la causa del riesgo (intrusiones, ataques y virus), su cobertura es limitada si no se complementa con mecanismos de monitoreo, respuesta proactiva y revisión periódica de configuraciones de seguridad. Por lo anterior se recomienda aumentar la frecuencia de verificación del estado del firewall y antivirus, con generación de reportes técnicos, implementar un sistema de monitoreo continuo que permita verificar el estado

operativo de los mecanismos de seguridad, actualizaciones automáticas, eventos bloqueados y reglas activas, ampliar el alcance del control para incluir no solo el licenciamiento, sino también la evaluación de configuraciones, políticas activas y gestión de alertas, realizar escaneo de vulnerabilidades y remediación de brechas de seguridad detectadas, y seguimiento a eventos e incidentes.

Evaluación efectividad control No 5:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Infraestructura de servidores y almacenamiento contratada en nube privada	
Causa del riesgo	Vencimiento de los contratos de nube privada y conectividad
Control definido	El Profesional Especializado de la Dirección Administrativa y Financiera - Gestión de TIC, tres meses antes de la finalización de cada contrato suscrito para la adquisición de servicios de nube privada y conectividad, iniciará el proceso para la nueva contratación de esos servicios elaborando el documento de estudios previos para radicación en Contratos, en caso de no adelantar el proceso los tiempos de transición entre el proveedor saliente y el proveedor entrante puede generar interrupción de los servicios. Como evidencia quedará el documento de estudios previos.
Tipo de control	Preventivo. Busca anticiparse al vencimiento de servicios tecnológicos esenciales asegurando continuidad operativa mediante una contratación oportuna.
Naturaleza	Manual. Depende completamente de la acción oportuna del Profesional Especializado para elaborar y radicar los estudios previos.
Alineación con la causa	El control actúa directamente sobre la causa (vencimiento del contrato) al asegurar la activación oportuna del proceso de contratación, con tiempo para gestionar la transición, evaluación de proveedores y continuidad de los servicios.
Evaluación de atributos del control	
Claridad	Están definidos el responsable, el objeto, la acción específica (elaborar estudios previos) y el momento de ejecución (tres meses antes del vencimiento).
Diseño	El control se enfoca en una acción clave (inicio anticipado del proceso contractual), con un umbral de tiempo definido y evidencia concreta esperada. Permite prevenir directamente la causa del riesgo.
Aplicación	Según la evidencia, el proceso de contratación de servicios ha sido oportunamente planificado y ejecutado conforme a los plazos, evitando interrupciones en la operación tecnológica.
Frecuencia	Se activa sólo ante el vencimiento de cada contrato, pero su oportunidad es crítica.
Responsable	Claramente asignado al Profesional Especializado de Gestión de TIC, con rol activo en la planeación y gestión precontractual.
Evidencia	Existen estudios previos y documentación que demuestran ejecución anticipada y adecuada del control. Se evidencia continuidad del servicio.
Nivel de efectividad	Alta. El control se encuentra bien diseñado, debidamente documentado, alineado con la causa del riesgo e implementado con oportunidad suficiente para evitar la interrupción de servicios críticos en la nube. La existencia de estudios previos y la planificación contractual dentro del plazo estipulado evidencian una gestión proactiva por parte de Gestión TIC. Su ejecución contribuye directamente a la continuidad de los servicios y a la protección de los activos de información en ambientes contratados. Si bien el control es efectivo, debe mencionarse que su naturaleza es enteramente manual y que lo hace dependiente de la gestión individual del funcionario y de la trazabilidad documental.

El Control No. 5 demuestra un nivel de efectividad alto, dado que su diseño está orientado a anticipar el vencimiento de los contratos de nube privada y conectividad, permitiendo una adecuada planeación y ejecución de los procesos precontractuales. La evidencia disponible indica que Gestión TIC ha cumplido con la elaboración oportuna de los estudios previos y ha evitado interrupciones en la continuidad de servicios esenciales para el procesamiento y almacenamiento de información institucional. Este control se encuentra claramente definido en cuanto a

responsabilidad, momento de aplicación y tipo de evidencia esperada, y está alineado directamente con la causa del riesgo identificado. No obstante, su naturaleza manual lo hace susceptible a omisiones por fallas humanas o falta de seguimiento, por lo que se recomienda fortalecerlo mediante procedimientos estandarizados que aseguren su sostenibilidad en el tiempo.

Evaluación efectividad control No 6:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Infraestructura de servidores y almacenamiento contratada en nube privada	
Causa del riesgo	Incumplimiento de las condiciones contractuales
Control definido	El Profesional Especializado de la Dirección Administrativa y Financiera - Gestión de TIC con funciones de supervisor de los contratos de nube privada y conectividad, monitoreará mensualmente el servicio creando los casos de soporte requeridos para reportar los incidentes y fallas que se presenten con los servicios contratados, con el objetivo de realizar los descuentos respectivos en la facturación y en caso de fallas críticas escalar los casos a la Dirección Administrativa y financiera para tomar las decisiones pertinentes encaminadas a proteger la información. En caso de no tomar estas acciones se pueden presentar interrupciones de los servicios contratados. Como evidencia quedará el registro de los casos abiertos en las plataformas de soporte del CNMH y de los proveedores de los servicios.
Tipo de control	Detectivo. El control identifica fallas una vez ocurren, mediante la creación de casos de soporte y su trazabilidad, lo que permite aplicar correctivos y sanciones contractuales.
Naturaleza	Manual con soporte en plataformas. Si bien el reporte se realiza a través de plataformas digitales, el análisis, la creación del caso y la gestión del seguimiento son realizados manualmente por el supervisor del contrato.
Alineación con la causa	El control responde directamente a la causa "incumplimiento de condiciones contractuales" mediante el seguimiento a incidentes y la creación de casos que permiten activar acciones correctivas o sanciones contractuales. Se trata de una intervención directa sobre la fuente del riesgo.
Evaluación de atributos del control	
Claridad	El control especifica el responsable, la frecuencia (mensual), las acciones (monitorear, registrar, escalar), el propósito (descuentos y decisiones) y la evidencia (casos reportados).
Diseño	Establece una cadena lógica entre el monitoreo de la calidad del servicio, la gestión de soporte, la acción administrativa (descuentos) y la decisión gerencial en caso de fallas críticas.
Aplicación	El informe "Tikets o Incidentes presentados con el servicio de Nube Privada" de junio de 2025, muestra la trazabilidad de los casos creados en la plataforma del proveedor, incluidos incidentes con demoras en recuperación de máquinas virtuales y solicitudes no resueltas, lo cual refleja monitoreo activo y seguimiento técnico.
Frecuencia	La revisión es mensual, lo cual permite seguimiento continuo al cumplimiento del servicio.
Responsable	El control está formalmente asignado al Profesional Especializado de Gestión de TIC, en su calidad de supervisor de los contratos.
Evidencia	El documento "Tikets o Incidentes presentados con el servicio de Nube Privada" entregado registra los casos creados, las fechas, el tipo de afectación y el nivel de respuesta del proveedor, lo que valida la ejecución del control.
Nivel de efectividad	Alta. El control está bien definido y se ejecuta de forma regular. Se encuentra alineado directamente con la causa del riesgo y permite evidenciar fallas en el servicio de nube privada, generar acciones administrativas correctivas (como descuentos en facturación), y escalar incidentes críticos para salvaguardar la información institucional del CNMH. La evidencia disponible demuestra una aplicación efectiva durante el primer semestre de 2025, con registros detallados de casos abiertos, seguimiento técnico y observaciones sobre fallas recurrentes. Como limitaciones del control puede señalarse que, aunque la plataforma permite trazabilidad, el control depende de la acción manual del supervisor para identificar, clasificar y registrar los incidentes y no se evidencia una métrica para determinar la severidad de las fallas de forma objetiva.

El Control No. 6 presenta un nivel de efectividad alto, ya que se encuentra adecuadamente diseñado y ejecutado para mitigar el riesgo derivado del incumplimiento de las condiciones contractuales en la prestación de servicios en la nube privada. El control contempla el monitoreo mensual del servicio, la creación de casos de soporte ante fallas detectadas y el escalamiento de situaciones críticas a la Dirección Administrativa y Financiera. La evidencia aportada demuestra la trazabilidad de los incidentes gestionados, así como una supervisión activa por parte Gestión de TIC. Este control permite generar alertas tempranas, respaldar descuentos en la facturación y adoptar decisiones orientadas a proteger los activos de información del CNMH. No obstante, su naturaleza manual y la ausencia de criterios de clasificación de incidentes representan oportunidades de mejora que podrían abordarse mediante herramientas complementarias de análisis, automatización y definición de métricas de criticidad que permitan calificar objetivamente las fallas y definir acciones automáticas de escalamiento o penalización.

Evaluación efectividad control No 7:

Riesgo: Pérdida de la integridad, disponibilidad y confidencialidad de la información **Activo de información:** Infraestructura de servidores y almacenamiento contratada en nube privada	
Causa del riesgo	Falta de presupuesto.
Control definido	El Profesional Especializado de la Dirección Administrativa y Financiera - Gestión de TIC anualmente gestionará el respectivo proyecto de inversión y plan de adquisiciones previendo los recursos económicos anuales y las respectivas vigencias futuras con el fin de prever oportunamente los recursos para la contratación de los servicios de nube privada y conectividad contratación durante la vigencia del proyecto respectivo. En caso de no gestionar adecuadamente el proyecto de inversión y plan de adquisiciones se tendrán períodos sin la prestación de los servicios respectivos.
Tipo de control	Preventivo. Tiene el propósito de anticipar la disponibilidad de recursos financieros, evitando interrupciones por falta de apropiación presupuestal oportuna.
Naturaleza	Manual. Depende de la gestión del profesional de la Dirección Administrativa y Financiera - Gestión de TIC a través de registros en sistemas institucionales (Plan Anual de Adquisiciones - PAA y proyectos de inversión).
Alineación con la causa	La gestión del proyecto de inversión y del PAA actúa directamente sobre la causa (falta de presupuesto), al prever los recursos con suficiente anticipación. La inclusión de vigencias futuras es clave para cubrir necesidades que exceden el año fiscal.
Evaluación de atributos del control	
Claridad	El control especifica el responsable, la acción (gestionar PAA y proyecto de inversión), la frecuencia (anual) y su propósito.
Diseño	Se enfoca en prevenir la causa raíz del riesgo (falta de recursos), actuando sobre el ciclo de planeación presupuestal y contractual del CNMH. Incluye acciones concretas como inclusión en el PAA y previsión de vigencias futuras.
Aplicación	El archivo "R2. Control 3 PAA-TIC" entregado, evidencia que los procesos de contratación TIC fueron incluidos en el Plan Anual de Adquisiciones 2025, con fechas estimadas, montos y fuentes de financiación, lo cual sugiere cumplimiento del control.
Frecuencia	Se ejecuta una vez por vigencia fiscal, pero con un impacto estratégico alto.
Responsable	El control está formalmente asignado al Profesional Especializado Gestión de TIC, en su rol articulador con las áreas financieras y contractuales.
Evidencia	El documento "R2. Control 3 PAA-TIC" detalla múltiples adquisiciones relacionadas con TIC, su programación y asignación presupuestal, lo que respalda su gestión anticipada.
Nivel de efectividad	Alta. El control se encuentra adecuadamente formulado y ejecutado. Está orientado a prevenir la falta de recursos financieros que puedan comprometer la continuidad de los servicios en la nube. La evidencia demuestra su aplicación, al haberse incluido de forma anticipada los contratos TIC en el PAA 2025, con soporte en fuentes de financiación identificadas y cronograma previsto. Esto denota una gestión responsable y articulada con el ciclo presupuestal institucional.

El Control No. 7 presenta un nivel de efectividad alto, dado que se encuentra adecuadamente formulado, está alineado directamente con la causa del riesgo identificada (falta de presupuesto), y su ejecución ha sido evidenciada a través del registro de contrataciones TIC en el Plan Anual de Adquisiciones (PAA) 2025. Este control permite prever de manera oportuna los recursos económicos necesarios para garantizar la continuidad de los servicios tecnológicos contratados en la nube privada, incluyendo la programación de vigencias futuras. La planificación financiera reflejada en el PAA evidencia un manejo anticipado y ordenado, lo cual reduce significativamente el riesgo de interrupciones por indisponibilidad presupuestal; sin embargo, al tratarse de un control de naturaleza manual, su efectividad sigue dependiendo de la gestión individual del responsable y de la coordinación oportuna con las áreas de planeación y presupuesto. En ese sentido, se recomienda complementarlo con procedimientos estandarizados que fortalezcan su sostenibilidad y trazabilidad.

La evaluación de los siete (7) controles definidos para mitigar el riesgo de pérdida de la integridad, disponibilidad y confidencialidad de la información en el CNMH evidencia una gestión parcial que, si bien cuenta con elementos positivos en términos de diseño y responsabilidad asignada, presenta limitaciones relevantes en su ejecución, cobertura y alineación con las causas específicas del riesgo.

En términos generales, se identificó que la mayoría de los controles son de naturaleza manual y dependen en gran medida de la acción individual del Profesional Especializado de Gestión de TIC, sin contar con mecanismos automatizados de verificación, alertas o integración con sistemas de seguimiento. Esta condición los hace vulnerables a omisiones, errores humanos o desactualización.

Los resultados reflejan que cuatro controles alcanzan un nivel de efectividad alto, dado que están bien diseñados, alineados c
on la causa que pretenden mitigar y presentan evidencia clara de aplicación; sin embargo, tres controles obtuvieron calificación moderada debido a debilidades en su cobertura, frecuencia o alcance operativo.

Adicionalmente, se identificó que la alineación entre algunos controles y las causas de riesgo es parcial, ya que algunos se limitan a reportar o monitorear condiciones sin intervenir directamente sobre la fuente del riesgo, como es el caso de los controles ambientales del centro de datos o la verificac
ión del licenciamiento de seguridad.

Este panorama evidencia la necesidad de:

- Fortalecer el diseño integral de los controles, el cual nace de la correcta y completa identificación de los riesgos de seguridad de la información, incorporando componentes tecnológicos, métricas de desempeño y validaciones funcionales.
- Desagregar el tratamiento de los riesgos por criterio afectado (confidencialidad, integridad y disponibilidad).
- Actualizar el Plan de Acción para el fortalecimiento de los controles.

- Establecer un modelo de seguimiento que permita revisar periódicamente la ejecución, eficacia y pertinencia de cada control en función del entorno de amenazas y los cambios operacionales.

En síntesis, aunque el CNMH ha avanzado en la definición formal de controles para la gestión de riesgos de seguridad de la información, existe margen de mejora para lograr una protección efectiva, sostenible y adaptativa de los activos digitales estratégicos de la entidad, como se ha indicado anteriormente comenzando por la correcta y completa identificación de los riesgos.

Observaciones al Informe Preliminar por parte de DAyF Gestión TIC

El 31 de julio de 2025, Control Interno envió el informe preliminar y en respuesta la DAyF – Gestión TIC presentó algunas observaciones, las cuales fueron revisadas y atendidas por Control Interno mediante respuesta remitida a través de correo electrónico el 15 de agosto de 2025, en los siguientes términos:

1. *Referencia al procedimiento "Respaldo y Recuperación de la Información" El procedimiento fue mencionado en el contexto del análisis debido a su relevancia para la gestión de continuidad y protección de la información; sin embargo, es correcto precisar que actualmente no se encuentra registrado como control en la matriz de riesgos. En consecuencia, se encuentra en proceso de actualización y revisión para su incorporación en la matriz de riesgos digitales, a fin de asegurar su alineación con los controles establecidos y la trazabilidad correspondiente.*

Respuesta de Control Interno: En el marco de la evaluación, se consideró pertinente hacer referencia al procedimiento "Respaldo y Recuperación de la Información" debido a que constituye un componente crítico para la gestión de continuidad, la recuperación ante incidentes y la protección de la información del CNMH, todos ellos elementos esenciales dentro del SGSI. Aunque actualmente este procedimiento se encuentra en proceso de actualización y aún no ha sido incorporado formalmente como control en la matriz de riesgos digitales, su mención en el análisis responde a la necesidad de reconocer su relevancia y anticipar la importancia de que su versión definitiva esté alineada con los controles establecidos. De esta forma, se promueve que, una vez actualizado, cuente con trazabilidad y seguimiento sistemático como parte de la gestión de riesgos de seguridad de la información.

2. *Evaluación del nivel de madurez frente al mapa de riesgos Para la revisión del nivel de madurez de la seguridad, consideramos que la metodología debía sustentarse en estándares técnicos como la ISO/IEC 27001 y las guías del MinTIC relacionadas con el Modelo de Seguridad y Privacidad de la Información (MSPI). Por lo anterior, estimamos que no resulta procedente emplear como referencia principal la guía del "Rol de las Unidades u Oficinas de Control Interno", dado que no está enfocada en la evaluación técnica de controles de seguridad de la información.*

Respuesta de Control Interno: Como mencionamos anteriormente Control Interno puede adelantar evaluaciones independientes y con criterios técnicos reconocidos, por lo cual el seguimiento se realizó de acuerdo con dos guías oficiales del DAFP que son complementarias:

En primer lugar, la Guía del Rol de las Unidades u Oficinas de Control Interno, la cual define las cinco etapas progresivas de madurez (Inicial, Repetible, Definido, Administrado y Optimizado) y orienta a las Oficinas de Control Interno en la evaluación de procesos, incluyendo la gestión del riesgo, en segundo lugar tenemos la Guía para la Administración del Riesgo (Versión 6, 2022) que establece el marco metodológico para identificar, analizar, valorar, tratar y hacer seguimiento a los riesgos en las entidades públicas de igual forma aplica a todos los tipos de riesgo, incluyendo los de seguridad de la información, por lo cual son referentes y metodologías ampliamente aceptadas dentro de la gestión pública.

Teniendo en cuenta lo anterior, la metodología utilizada no sustituye los estándares técnicos como ISO/IEC 27001 o las guías MinTIC, sino que aplica el marco exigido para la función de Control Interno en entidades públicas. De hecho, ambas guías del DAFP trabajan de la mano:

- La Guía del Rol da el criterio de madurez.
- La Guía de Administración del Riesgo aporta la metodología de gestión sobre la cual se mide dicha madurez.

De otro lado, la evaluación de control interno se centró en el proceso de gestión de riesgos de seguridad de la información con un enfoque objetivo, normativamente respaldado y alineado con el MIPG, sin excluir la posibilidad de integrar criterios técnicos de ISO/IEC 27001 y MSPI en etapas posteriores.

3. *Enfoque de la gestión de riesgos. Reiteramos que, para la administración de riesgos en el ámbito TIC, es fundamental que el análisis se centre específicamente en los riesgos de seguridad de la información y no en una gestión de riesgos general. Ello permite una evaluación alineada con las amenazas, vulnerabilidades y controles propios del SGSI.*

Respuesta de Control Interno: Todo el informe se enfocó en el análisis de los riesgos de seguridad de la información (incluidos los digitales), y en el informe en ninguno de sus apartes se menciona, analiza, ni evalúa ningún riesgo identificado por el CNMH con tipologías diferentes (gestión, corrupción, fiscales).

4. *Criterios de evaluación del nivel de madurez del proceso. Contrario a lo señalado, sí existe un marco definido para la gestión de seguridad de la información: la norma ISO/IEC 27001, que es la base formal del sistema de gestión adoptado por la Entidad.*

Respuesta de Control Interno: En la descripción del nivel de madurez (tabla Número 2), cuando se señala que "No existe un marco definido" se está haciendo alusión a la etapa "Inicial" del nivel de madurez; sin embargo, al evaluar la totalidad de los criterios definidos dentro del proceso de gestión de riesgos de seguridad de la información del CNMH se observó que se encuentra en la etapa de madurez "Definido", es decir, que "El proceso está formalizado en políticas y procedimientos. Se aplica con regularidad. Hay responsables definidos y herramientas básicas para seguimiento", por tanto, lo argumentado por el Grupo de TI no coincide con lo reportado en el informe de seguimiento remitido por Control Interno.

5. *En cuanto al control de mantenimiento de equipos cada seis (6) meses, confirmamos que la periodicidad establecida es correcta y está respaldada por las actividades técnicas que realiza el equipo de TIC - Mesa de Ayuda.*

Respuesta de Control Interno: Dado que no se precisa a qué control se hace referencia, se asume que la respuesta corresponde a los controles 1 y 2 por la frecuencia de estos dentro del mapa de riesgos de seguridad de la información. Frente al particular el resultado de la evaluación del control se ubicó en un nivel moderado, por la baja frecuencia y dependencia de reporte humano, lo cual limita su efectividad preventiva, de ahí la recomendación de la revisión de su frecuencia por el impacto que podría tener en caso de materialización; sin embargo, el Grupo TIC tiene la autonomía de evaluar la recomendación para acogerla o no.

Control Interno agradece la colaboración y disposición del Grupo TIC durante el desarrollo del seguimiento al mapa y/o matriz de riesgos de seguridad de la información, en el marco de nuestro rol como tercera línea de defensa, reiteramos nuestra disposición para trabajar de manera articulada con Gestión TIC, con el fin de fortalecer los procesos de gestión del riesgo y la seguridad de la información en la entidad.

CONCLUSIÓN

El seguimiento realizado al mapa de riesgos de seguridad de la información del CNMH, permite concluir que la entidad ha logrado avances significativos en la formalización, publicación e implementación de acciones para el tratamiento de riesgos tecnológicos y digitales. El mapa de riesgos vigente contiene controles definidos, ejecutados y documentados por el área DAyF-Gestión TIC; sin embargo, el documento evaluado contempla un único riesgo asociado a dos activos de información, sin considerar otras áreas críticas, procesos o servicios que también pueden ser vulnerables a amenazas de seguridad digital, lo que limita el alcance y efectividad del proceso de gestión del riesgo.

Se evidenció que el mapa de riesgos de seguridad de la información del CNMH agrupa varios eventos de riesgo en una única línea, combinando criterios de confidencialidad, integridad y disponibilidad. Esta práctica dificulta la trazabilidad, priorización y definición específica de controles, lo que afecta la eficacia del tratamiento del riesgo.

No obstante, el proceso de gestión de riesgos de seguridad se encuentra en una etapa de madurez "Definida", lo cual indica que, si bien existe una estructura institucional y metodológica establecida, aún se requiere fortalecer la trazabilidad, la participación transversal de las dependencias, la formalización de decisiones sobre el riesgo residual y la integración con los procesos de planeación y toma de decisiones estratégicas.

En cuanto a la efectividad de los controles, algunos de ellos no abordan directamente las causas de los riesgos identificados, lo que reduce su capacidad preventiva o correctiva. En varios casos, los controles están enfocados en el seguimiento o la generación de reportes, sin acciones que intervengan sobre la fuente del riesgo.

RECOMENDACIONES

- Se recomienda fortalecer el proceso de identificación de riesgos de seguridad de la información, ampliando el análisis de amenazas y vulnerabilidades a la totalidad de los activos de información, procesos misionales, de apoyo y áreas estratégicas del CNMH, incluyendo servicios tercerizados y recursos tecnológicos críticos. Este fortalecimiento debe realizarse en concordancia con lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, asegurando un enfoque integral y actualizado.

  La implementación de esta recomendación permitirá incrementar la cobertura del mapa de riesgos de seguridad de la información, mejorar la detección oportuna de vulnerabilidades, alinear la gestión con los principios de confidencialidad, integridad y disponibilidad, y facilitar el monitoreo efectivo del cumplimiento de las políticas internas de seguridad de la información. Así mismo, contribuirá a una toma de decisiones más informada y a la consolidación de una cultura de gestión del riesgo basada en evidencia.

- Se recomienda incluir en el mapa de riesgos de seguridad de la información, los riesgos asociados a los procesos y procedimientos (como por ejemplo del procedimiento "Respaldo y Recuperación de la Información", código GTC-PR-007, versión 2), identificando de manera específica las amenazas que puedan afectar el cumplimiento de su objetivo, en especial aquellas relacionadas con *la pérdida*, accesibilidad, uso y protección de la información, para la operación de todos los procesos institucionales. Así mismo, se sugiere definir e implementar los controles necesarios que garanticen la protección, disponibilidad y restauración de la información, fortaleciendo así la capacidad de respuesta ante incidentes y la continuidad operativa del CNMH.

- Se recomienda formalizar la aceptación del riesgo residual a través de mecanismos documentales claros y verificables, tales como actas de comité de dirección, comités de riesgos, resoluciones internas u otros medios institucionales que evidencien la decisión consciente y fundamentada de asumir el riesgo identificado. Esta práctica no solo fortalece la trazabilidad y transparencia del proceso de gestión del riesgo, sino que además garantiza la responsabilidad compartida entre las áreas involucradas, facilitando el monitoreo, la revisión periódica y la implementación de medidas adicionales en caso de cambios en el nivel de exposición o en el entorno de la entidad.

- Se recomienda corregir los errores técnicos identificados en el mapa de riesgos de seguridad de la información, tales como campos vacíos, celdas con valores inconsistentes o errores de referencia (por ejemplo, '#N/D'), con el fin de garantizar la integridad y confiabilidad de la información consignada.

- Se recomienda fortalecer el uso transversal de la matriz de riesgos de seguridad de la información, promoviendo su integración efectiva en los diferentes niveles y procesos institucionales, tales como la planeación estratégica y operativa, la formulación presupuestal, la evaluación institucional, la contratación, y la toma de decisiones administrativas y técnicas.

Este enfoque permitirá que la gestión del riesgo no se limite a un ejercicio técnico o documental, sino que se consolide como una herramienta de apoyo real para la dirección y el cumplimiento de los objetivos institucionales, garantizando que los riesgos de seguridad digital sean gestionados de forma anticipada, sistemática y articulada con los instrumentos de gestión del CNMH. Además, su uso transversal contribuye a una cultura organizacional más consciente y proactiva frente a la protección de los activos de información y al fortalecimiento del modelo de seguridad de la información.

- Dar continuidad a la ejecución del plan de acción elaborado por la DAyF- Gestión TIC, asegurando su implementación gradual y alineación con el SIG, la ISO/IEC 27001:2022, la ISO/IEC 27005 y el MSPI (Resolución 02277 de 2025 de MinTIC, numeral 7.3.2.).

- Se recomienda evaluar la posibilidad de implementar gradualmente herramientas tecnológicas especializadas adicionales en relación con la gestión de seguridad de la información, que permitan monitorear en tiempo real la ejecución y desempeño de los controles definidos, así como emitir alertas automáticas ante desviaciones, fallas o incumplimientos, facilitando la trazabilidad completa de las acciones correctivas y preventivas adoptadas. Su adopción fortalecerá la capacidad institucional para anticipar riesgos, responder oportunamente a incidentes de seguridad y mantener evidencia objetiva sobre la eficacia de los controles aplicados, en línea con los principios de mejora continua y lo establecido en la Guía para la Administración del Riesgo.

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

No	DESCRIPCION DEL HALLAZGO	RECOMENDACION

FIRMAS RESPONSABLES

Evaluadores:

Willson Ernesto Albarracin Gómez – Contratista Control Interno

Vo. Bo.

Doris Yolanda Ramos Vega - Asesora de Control Interno