CI2026303099
19-10-2026 14:51:43
Radicador: CARLOS ALBERTO TORO MEJIA

MEMORANDO

1400

FECHA: Medellín, 19 de octubre de 2026

PARA:**JUAN DAVID GOMEZ FLOREZ**
RECTOR DE INSTITUCIÓN UNIVERSITARIA
RECTORÍA

DE:CARLOS ALBERTO TORO MEJIA
JEFE DE OFICINA

ASUNTO: Remisión informe definitivo auditoría legal de seguimiento al Modelo de Seguridad y Privacidad de la Información – MSPI Vigencia 2026.

Con fundamento en Ley 87 de 1993 y la Resolución No. 089 del 29 de abril de 2020, por medio de la cual se actualiza el Manual de Auditoría Interna para La Institución Universitaria Colegio Mayor de Antioquia y el plan general de auditoría, aprobado por el Consejo Directivo de la Institución, en acta No. 005 de la sesión ordinaria del 24 de abril de 2026, me permito hacer entrega del informe definitivo correspondiente a la auditoría de legal de seguimiento al Modelo de Seguridad y Privacidad de la Información – MSPI Vigencia 2026, que se practicó por parte de la Oficina de Evaluación y Control de la Institución.

La auditoría se llevó a cabo de acuerdo al proceso de control interno vigente actualmente para la Institución Universitaria Colegio Mayor de Antioquia, es decir, se comunicaron los

VIGILADA por el Ministerio de Educación Nacional

resultados obtenidos con los responsables de la unidad auditable al interior de la Institución.

Para la presente auditoría se requirió elaboración del Plan de Mejoramiento.

Atentamente,

CARLOS ALBERTO TORO MEJIA
JEFE DE OFICINA
OFICINA DE EVALUACIÓN Y CONTROL

Anexos: (25)folios

VIGILADA por el Ministerio de Educación Nacional

INFORME DE AUDITORÍA

CONTROL INTERNO







WWW.COLMAYOR.EDU.CO

CÓDIGO: CI-FR-001
VERSIÓN: 010
FECHA: 06/09/2022

NIT: 890980134-1

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

INFORME FINAL

AUDITORÍA LEGAL DE SEGUIMIENTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI 2026

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA

Equipo de trabajo

CARLOS ALBERTO TORO MEJÍA
JEFE OFICINA EVALUACIÓN Y CONTROL

ANDERSSON BENITEZ ARBOLEDA
PROFESIONAL OFICINA EVALUACIÓN Y CONTROL

OFICINA DE EVALUACIÓN Y CONTROL

Medellín

Octubre 15 de 2026

Contenido

PRESENTACIÓN 6
1. ALCANCE DE LA AUDITORÍA 7
2. RIESGOS ASOCIADOS A LA UNIDAD AUDITABLE 7
Tabla 1 Riesgos Asociados 7
3. CRITERIOS DE AUDITORÍA 8
Tabla 2 Criterios 8
4. OBJETIVOS 8
4.1 OBJETIVO GENERAL 8
4.2 OBJETIVOS ESPECÍFICOS 8
5. METODOLOGÍA 9
6. LIMITACIONES 9
7. MUESTRA 9
8. RESUMEN 10
9. RESULTADOS DE LA AUDITORÍA 11
9.1 Estructura documental para la gestión de seguridad y privacidad de la información 11
9.2 Seguimiento a indicadores – Plan de Mejoramiento N.°063 11
9.3 Gestión de riesgos y efectividad de controles 11
9.4 Gestión de incidentes de seguridad digital 12
9.5 Copias de seguridad y administración de accesos 12
9.6 HALLAZGOS 13
9.6.1 Hallazgo 1 – Fortalecimiento de la trazabilidad de activos de información, controles aplicables y diagnóstico del MSPI 13
9.6.2 Hallazgo 2 – Verificación de la ejecución y resultados de pruebas de continuidad y recuperación 14
9.6.3 Hallazgo 3 – Trazabilidad de la ejecución de capacitación y sensibilización en seguridad y privacidad 15
9.7 Composición del riesgo y Evaluación puntos de control 15
10. CONCLUSIONES 22
11. RECOMENDACIONES 22
12. GLOSARIO 24
13. ANEXOS 24
14. BIBLIOGRAFÍA 24

Lista de tablas

Tabla 1 Riesgos Asociados 7
Tabla 2 Criterios 8
Tabla 3 Síntesis Ejecutiva de la Auditoría 10
Tabla 4 Atributos para el diseño del control del riesgo 17

Lista de ilustraciones

Ilustración 1Composición del riesgo 16
Ilustración 2 Matriz inherente de calor - nivel de severidad 20
Ilustración 3 Matriz de calor residual – nivel de severidad de los controles identificados 21

PRESENTACIÓN

Con fundamento en la Ley 87 de 1993, el Manual de Auditoría Interna de la Institución Universitaria Colegio Mayor de Antioquia y el Plan General de Auditoría – PGA de la vigencia 2026, la Oficina de Evaluación y Control realizó la auditoría al Modelo de Seguridad y Privacidad de la Información – MSPI, con el propósito de evaluar los principales elementos de implementación, operación, seguimiento y mejora del modelo, a partir de la evidencia suministrada y disponible durante el ejercicio auditor.

La auditoría tomó como antecedente el informe de la vigencia 2025, en el cual se identificaron oportunidades relacionadas, entre otros aspectos, con la aplicación y actualización del Plan de Seguridad y Privacidad de la Información y con la medición de indicadores de evaluación y desempeño. Para 2026, la revisión se orientó a determinar no solo la existencia documental de instrumentos, sino la evidencia de su aplicación, seguimiento y efectividad.

Para el desarrollo de esta auditoría se aplicaron diferentes técnicas de auditoría, como consulta, análisis y seguimiento a la información suministrada por el auditado.

Finalmente, como resultado de la presente auditoría, se considera importante establecer y fortalecer las acciones, métodos, procedimientos y mecanismos de prevención, corrección, evaluación y mejoramiento continuo que resulten pertinentes, con el propósito de contribuir al adecuado desarrollo del proceso y garantizar el cumplimiento de las disposiciones legales y demás normativas aplicables en la materia.

1. ALCANCE DE LA AUDITORÍA

La auditoría comprendió la revisión de los principales componentes del MSPI durante la vigencia 2026, incluyendo el Plan de Seguridad y Privacidad de la Información, indicadores, gestión de riesgos, activos de información, controles de acceso, gestión de incidentes, copias de seguridad, continuidad y recuperación, capacitación y sensibilización, documentación del proceso y seguimiento a acciones de mejoramiento. La información de vigencias anteriores se utilizó únicamente como antecedente y elemento de trazabilidad.

La auditoría considerará la verificación de la implementación de las 5 fases del modelo:
- Diagnostico.
- Planificación.
- Operación.
- Evaluación de desempeño.
- Mejoramiento continuo.

2. RIESGOS ASOCIADOS A LA UNIDAD AUDITABLE

Estos riesgos fueron identificados en la matriz de riesgos de gestión con corte a 30 de abril de 2026, publicado en la página web institucional en el siguiente link: https://www.colmayor.edu.co/institucional/planeacion-institucional/planeacion-institucional-7/

Tabla 1 Riesgos Asociados

Tipo de Riesgo	Nombre del Riesgo	Controles Principales	Escenario de Riesgo (MSPI)
Gestión	**Ciberseguridad**	El administrador del Data Center configura la Plataforma Tecnológica que permite realizar redundancia a aplicativos Institucionales y Red de Datos de tal manera que, si falla un servidor, el otro entra a funcionar y se verifican los indicadores.	Aplican para la auditoría legal al Modelo y seguridad de la información vigencia 2026

Fuente: https://www.colmayor.edu.co/institucional/planeacion-institucional/planeacion-institucional-7/

3. CRITERIOS DE AUDITORÍA

Para el desarrollo de la auditoría se tomaron como criterios de evaluación las disposiciones legales, reglamentarias, técnicas e institucionales aplicables al Modelo de Seguridad y Privacidad de la Información – MSPI, así como los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y la documentación adoptada por la Institución para la gestión de la seguridad y privacidad de la información. Estos criterios constituyeron el marco de referencia para contrastar la información y las evidencias disponibles, evaluar la implementación y operación de los controles y determinar el grado de aplicación de los mecanismos establecidos para proteger la confidencialidad, integridad y disponibilidad de la información, así como para gestionar los riesgos de seguridad digital, la continuidad de los servicios y el mejoramiento continuo del modelo.

Tabla 2 Criterios

CRITERIOS
Resolución 00500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
Acuerdo 09 de 2018 (interna) “Por medio de la cual se adopta la Política de Seguridad y Privacidad de la Información de la Institución Universitaria Colegio Mayor de Antioquia”.
Decreto 2106 de 2019, “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública”

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI por parte de la Institución Colegio Mayor de Antioquia.

4.2 OBJETIVOS ESPECÍFICOS

- Verificar la aplicación de las fases del modelo por parte de la institución.
- Evaluar la efectividad de los controles dispuestos por parte de la Institución para evitar o mitigar la materialización de los riesgos de seguridad de la información.

5. METODOLOGÍA

Para el desarrollo de la auditoría se aplicó una metodología basada en la revisión, análisis y contraste de la información y las evidencias disponibles, orientada a determinar el nivel de implementación y operación de los principales componentes del Modelo de Seguridad y Privacidad de la Información – MSPI. El ejercicio auditor combinó la revisión documental y normativa con el análisis de planes, procedimientos, matrices, registros y demás soportes suministrados por el área responsable, procurando establecer la correspondencia entre los lineamientos formalmente definidos por la Institución y su aplicación efectiva. La evaluación se desarrolló bajo un enfoque basado en riesgos, considerando no solamente la existencia de documentos y controles, sino también, cuando la evidencia disponible lo permitió, aspectos relacionados con su ejecución, oportunidad, trazabilidad, seguimiento y capacidad para contribuir a la mitigación de los riesgos asociados con la seguridad y privacidad de la información.

6. LIMITACIONES

Durante la auditoría se solicitó información complementaria. Con posterioridad al preinforme, el proceso auditado aportó doce archivos adicionales que fueron incorporados al análisis: documentación del MSPI, plan de tratamiento de riesgos, inventario consolidado, procedimientos de incidentes y antivirus, manual de respaldos y recuperación, documentación de sistemas, convocatoria de copias de seguridad y cuatro convocatorias de pruebas de planta eléctrica. Esta entrega amplió el soporte documental y exigió revisar las valoraciones preliminares.

El inventario recibido contiene 2.371 registros de datos en la hoja 'Consolidado', además de su encabezado, y campos de descripción, placa, responsable, categoría y custodio. Su contenido evidencia un registro de bienes y recursos; no se constató, con esa sola estructura, una clasificación integral de activos de información por criterios de seguridad. Tampoco se identificó en el paquete una Declaración de Aplicabilidad individualizada ni resultados técnicos de restauración o recuperación.

7. MUESTRA

La muestra fue no estadística y dirigida por criticidad. Comprendió los documentos y evidencias disponibles sobre el Plan de Seguridad y Privacidad de la Información, riesgos y controles de seguridad digital, procedimientos de incidentes, respaldos, accesos, continuidad,

documentación tecnológica, indicadores y acciones de mejoramiento, complementados con la información solicitada al área responsable.

8. RESUMEN

Como resultado de la evaluación realizada, se identificaron fortalezas, avances y oportunidades de fortalecimiento en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI. De manera general, la Institución dispone de instrumentos documentales, procedimientos y controles orientados a la gestión de la seguridad y privacidad de la información; no obstante, la auditoría evidenció aspectos que requieren continuar fortaleciéndose, principalmente en relación con la trazabilidad entre los instrumentos definidos y las evidencias de su implementación, seguimiento y efectividad. Asimismo, para algunos componentes no fue posible efectuar una verificación integral debido a que, al cierre del ejercicio auditor, no se contó con la totalidad de la información y los soportes requeridos, situación que fue considerada en la valoración de los resultados y que se desarrolla específicamente en el apartado de limitaciones del presente informe.

Tabla 3 Síntesis Ejecutiva de la Auditoría

Componente	Valoración	Síntesis
Plan de Seguridad y Privacidad	Cumple con oportunidades de mejora	Se evidenció estructura documental; se requiere fortalecer trazabilidad de ejecución, medición y seguimiento.
Indicadores / Plan 063	En seguimiento	Situación previamente identificada; no se formula una observación nueva para evitar duplicidad.
Riesgos de seguridad y privacidad	Cumple con oportunidades de mejora	Se identificó gestión institucional de riesgos; la efectividad debe sustentarse en la operación de controles, no solo en ausencia de materialización.
Gestión de incidentes	Cumple documentalmente	Existe el procedimiento GT-PR-014. Según la información suministrada, no se reportaron incidentes en el período evaluado.
Accesos	Cumple con evidencia disponible	Se identificó documentación institucional para administración de cuentas y accesos; la conclusión se limita a la evidencia aportada.
Copias de seguridad	Cumple con evidencia disponible	Existe marco documental para respaldos y recuperación; la verificación integral de pruebas y resultados quedó limitada por la evidencia disponible.
Continuidad y recuperación	Requiere fortalecimiento	No se contó con evidencia suficiente para acreditar integralmente actualización, formalización y pruebas periódicas de continuidad/recuperación.
Declaración de Aplicabilidad – SoA	No verificable integralmente	No se recibió evidencia suficiente para concluir sobre su estado y aplicación durante la vigencia.

Componente	Valoración	Síntesis
Activos de información	No verificable integralmente	La evidencia disponible no permitió verificar de forma suficiente inventario, clasificación, responsables y actualización.
Capacitación y sensibilización	No verificable integralmente	No se recibió evidencia suficiente de ejecución y cobertura de actividades específicas de seguridad y privacidad durante 2026.
Diagnóstico / línea base MSPI	No verificable integralmente	No se recibió evidencia suficiente para establecer el resultado actualizado de avance o madurez del modelo.

9. RESULTADOS DE LA AUDITORÍA

9.1 Estructura documental para la gestión de seguridad y privacidad de la información

Como aspecto favorable, se evidenció que la Gestión de Tecnología y Medios Audiovisuales dispone de una estructura documental que incluye, entre otros, el Plan de Seguridad y Privacidad de la Información GT-MA-006, el Plan de Tratamiento de Riesgos GT-MA-004, el Manual de backups y recuperación de desastres GT-MA-002 y procedimientos relacionados con copias de seguridad, administración de cuentas de usuario y gestión de incidentes de seguridad digital. Esta estructura constituye una base para la estandarización de controles y la aplicación del ciclo de gestión del MSPI.

No obstante, la existencia documental no sustituye la necesidad de acreditar periódicamente su aplicación, medición y efectividad.

9.2 Seguimiento a indicadores – Plan de Mejoramiento N.°063

El informe de auditoría MSPI 2025 identificó la necesidad de fortalecer la medición y seguimiento de indicadores del Plan de Seguridad y Privacidad de la Información. Para la vigencia 2026 este asunto se encuentra vinculado al seguimiento del Plan de Mejoramiento N.°063. En consecuencia, la Oficina de Evaluación y Control no formula una nueva observación sobre el mismo hecho, con el fin de evitar duplicidad, y mantiene su verificación dentro del mecanismo institucional de seguimiento a planes de mejoramiento.

9.3 Gestión de riesgos y efectividad de controles

Se evidenció la existencia de riesgos institucionales asociados con seguridad y privacidad de la información y actividades de seguimiento durante 2026. La información disponible reportó

ausencia de materialización de los eventos objeto de seguimiento. Este resultado es favorable; sin embargo, desde la perspectiva de auditoría, la no materialización no constituye por sí sola evidencia suficiente de efectividad. La valoración debe complementarse con evidencia de ejecución, oportunidad, cobertura y capacidad de mitigación de los controles definidos.

Resultado: Cumple con oportunidades de mejora. Se recomienda mantener soportes consolidados que permitan demostrar la ejecución y resultados de los controles en cada período de seguimiento.

9.4 Gestión de incidentes de seguridad digital

Se verificó la existencia del procedimiento GT-PR-014 – Gestión de Incidentes de Seguridad Digital, versión 00 del 13 de mayo de 2025, que contempla actividades de detección, registro, clasificación, contención, análisis, recuperación, comunicación, cierre y revisión posterior del incidente. De acuerdo con la información suministrada durante la auditoría, no se reportaron incidentes de ciberseguridad durante el período evaluado.

La conclusión anterior se circunscribe a la información aportada y no constituye una certificación independiente de inexistencia de eventos. Se considera favorable contar con un procedimiento formal; su efectividad deberá continuar verificándose mediante registros y evidencias cuando se presenten eventos.

9.5 Copias de seguridad y administración de accesos

La documentación institucional revisada contempla procedimientos para copias de seguridad y administración de cuentas de usuario. Con la evidencia disponible se reconoce la existencia de controles formalizados; no obstante, la auditoría no contó con elementos suficientes para efectuar una validación técnica independiente de la totalidad de respaldos, restauraciones, permisos y ambientes. Por tanto, la valoración se limita a la evidencia documental aportada y no equivale a certificación técnica integral.

9.6 HALLAZGOS

9.6.1 Hallazgo 1 – Fortalecimiento de la trazabilidad de activos de información, controles aplicables y diagnóstico del MSPI

Condición: La información complementaria permitió acreditar la existencia de un inventario consolidado de bienes y recursos y de documentación institucional sobre el MSPI y el tratamiento de riesgos. Sin embargo, el inventario examinado no permite identificar de manera suficiente, por sí solo, la clasificación de activos de información y su vínculo con riesgos y controles; tampoco se identificó una Declaración de Aplicabilidad individualizada ni una medición verificable de línea base del modelo en la nueva entrega.

Criterio: El MSPI adoptado mediante la Resolución MinTIC 00500 de 2021 contempla un ciclo de diagnóstico, planificación, operación, evaluación de desempeño y mejoramiento continuo, que requiere información documentada y verificable para soportar la selección y aplicación de controles, la identificación de activos y el seguimiento al nivel de implementación del modelo.

Análisis: Se desvirtúa la afirmación preliminar de ausencia de inventario, pues se recibió un archivo consolidado. Subsiste una necesidad de articulación y trazabilidad entre los registros aportados, los activos de información sujetos a protección, los riesgos identificados, los controles seleccionados y el avance del MSPI. Esta conclusión no equivale a afirmar que esos instrumentos no existan fuera del conjunto de soportes revisado.

Efecto: Posibilidad de mantener controles sin una trazabilidad suficiente respecto de los activos y riesgos que protegen; dificultad para priorizar acciones de mejora; y limitaciones para demostrar el nivel de implementación y cumplimiento del MSPI ante ejercicios de seguimiento o evaluación.

Recomendación: Consolidar, actualizar y mantener disponible la documentación que soporte la Declaración de Aplicabilidad, el inventario y clasificación de activos de información y el diagnóstico o línea base del MSPI, definiendo responsables, periodicidad de actualización y mecanismos de aprobación y seguimiento.

9.6.2 Hallazgo 2 – Verificación de la ejecución y resultados de pruebas de continuidad y recuperación

Condición: La documentación disponible evidencia lineamientos relacionados con continuidad, respaldos y recuperación; se recibieron el manual de backups y recuperación, una convocatoria de copia de seguridad para el 30 de septiembre de 2026 y convocatorias de pruebas de planta eléctrica de los días 11, 18 y 25 de septiembre y 2 de octubre de 2026. Estos soportes acreditan lineamientos y programación de actividades, pero no contienen por sí mismos resultados de restauración de información, tiempos reales de recuperación, incidencias detectadas ni actas de ejecución y evaluación de pruebas integrales de continuidad.

Criterio: El MSPI requiere que la gestión de seguridad y privacidad incorpore mecanismos para preservar la disponibilidad de la información y la continuidad de los servicios, incluyendo planificación, implementación, evaluación y mejora de las medidas establecidas. La documentación institucional disponible contempla respaldos y recuperación como parte de la gestión tecnológica.

Análisis: La entrega adicional modifica favorablemente la valoración de existencia documental y de programación. No obstante, las pruebas de planta eléctrica se refieren a infraestructura de soporte y no sustituyen una prueba de recuperación de sistemas, servicios y datos. La valoración de efectividad requiere evidencias de ejecución, resultados, responsables, tiempos y tratamiento de desviaciones.

Efecto: Posible afectación de la disponibilidad y recuperación oportuna de servicios e información crítica ante fallas tecnológicas, incidentes o contingencias, así como dificultad para demostrar que las estrategias definidas funcionan dentro de los tiempos requeridos.

Recomendación: Formalizar o actualizar, según corresponda, los mecanismos institucionales de continuidad y recuperación ante desastres; establecer un cronograma periódico de pruebas; documentar resultados, responsables, desviaciones, lecciones aprendidas y acciones de mejora; y conservar evidencia verificable de su ejecución.

9.6.3 Hallazgo 3 – Trazabilidad de la ejecución de capacitación y sensibilización en seguridad y privacidad

Condición: En la información complementaria se identificaron lineamientos relacionados con concienciación y seguridad; sin embargo, no se aportaron registros individualizables de ejecución de actividades de capacitación y sensibilización específicas durante 2026, tales como programas ejecutados, contenidos, convocatorias con asistencia, evaluaciones o reportes de cobertura.

Criterio: El MSPI incorpora medidas de talento humano y cultura de seguridad como elementos necesarios para gestionar los riesgos asociados al uso y protección de la información. El antecedente de auditoría 2025 también da cuenta de acciones institucionales relacionadas con capacitación y comunicación en seguridad de la información.

Análisis: La documentación de política y planeación permite reconocer la previsión del control, pero no verificar su operación ni alcance durante 2026. La situación se formula como insuficiencia de evidencia disponible, sin concluir que no se hayan realizado capacitaciones.

Efecto: Incremento de la exposición a errores humanos, prácticas inseguras y respuestas inadecuadas frente a eventos de seguridad, así como dificultad para demostrar la apropiación institucional de los lineamientos del MSPI.

Recomendación: Ejecutar y documentar un programa periódico de capacitación y sensibilización en seguridad y privacidad de la información, definiendo población objetivo, contenidos, periodicidad, responsables, evidencias de participación y mecanismos de evaluación de apropiación o efectividad.

9.7 Composición del riesgo y Evaluación puntos de control

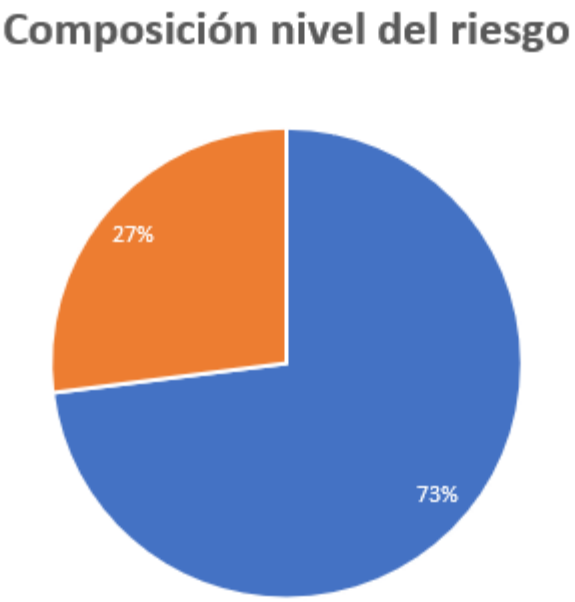
- **Composición del riesgo**

A continuación, se determina para la Institución Universitaria Colegio Mayor de Antioquia, el nivel de riesgo en relación al Modelo de Seguridad y Privacidad de la Información - MSPI de la vigencia 2026.

Información verificada con hallazgos que no alteran el resultado de la evaluación realizada.

Por lo tanto:

Ilustración 1Composición del riesgo



Elaboró: Profesional de la Oficina de Evaluación y Control.

Lo anterior y como se observa en la ilustración No.1, se encontró deficiencia en la entrega de la documentación suministrada y referida por parte del proceso de tecnología e informática y revisada en este ejercicio de auditoría.

Por lo anterior, el riesgo aceptable en un 73% y tolerable es del 27%, sobre el total de lo revisado.

A continuación, se realiza la evaluación de los controles identificados para esta unidad auditable:

- **Evaluación de los controles**

El Departamento Administrativo de la Función Pública -DAFP-, actualizó la guía para la gestión integral del riesgo en entidades públicas, versión 7, de agosto de 2025, observando la siguiente estructura para la descripción del control:

"(…) despliegue de los atributos para el control"[1]

"Responsable: Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (Directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control"[2]

"Acción: Determina para qué se realiza el control, se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar."[3]

"Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos: Documentación, Frecuencia, Evidencia, Ejecución[4]*".*

Para la unidad auditable tenemos el siguiente riesgo y sus controles:

Nombre del Riesgo: Ciberseguridad

Control 1: El administrador del Data Center configura la Plataforma Tecnológica que permite realizar redundancia a aplicativos Institucionales y Red de Datos de tal manera que, si falla un servidor, el otro entra a funcionar y se verifican los indicadores.

Tabla 4 Atributos para el diseño del control del riesgo

Valoración de controles					
Control	**Características**				**Peso**
Control 1	**Atributos de Eficiencia**	**Tipo**	**Preventivo**	X	25%
			Detectivo		

[1] file:///D:/Downloads/2025-09-11_Guia_gestion_integral_riesgo_v7.pdf
[2] Ídem del anterior
[3] Ídem del anterior
[4] Ídem del anterior

Valoración de controles					
Control	**Características**				**Peso**
			Correctivo		
		Implementación	**Automático**		
			Manual	X	15%
	Análisis atributos formalización del control				
	Atributos de Formalización del control	**Documentación**	**Procedimientos**		
			Sistemas de información		
			Otros esquemas	X	
		Frecuencia	**Siempre que se ejecuta la actividad**		
			Periódicamente (diario, mensual, bimestral, trimestral, semestral).	X	
		Evidencia	**Con Registro manual**	X	
			Con Registro electrónico		
		Ejecución	**Interna**	X	
			Externa		
			Mixta		
Total, valoración del control					**40%**

Fuente: guía para la gestión integral del riesgo en entidades públicas, versión 7 de 2025.
Elaboró: Profesional de la oficina de evaluación y control

La evaluación realizada al punto de control permitió determinar:

- El control es de carácter preventivo, es decir, el "*control accionado en la entrada del proceso y antes de que se realice la actividad generadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado*"[5]

- Se ejecuta de forma manual por parte de la dependencia de la Institución: "*es decir que los controles son ejecutados por personas*".[6]

[5] https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499
[6] Ídem al anterior

- Documentación otros esquemas: "*el control cuenta con políticas de operación, manuales o guías específicos".*[7]

- Su frecuencia es periódica: "*es decir, la oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riego de manera oportuna".*[8]

- Evidencia de su ejecución: en este punto se puede identificar la siguiente característica:

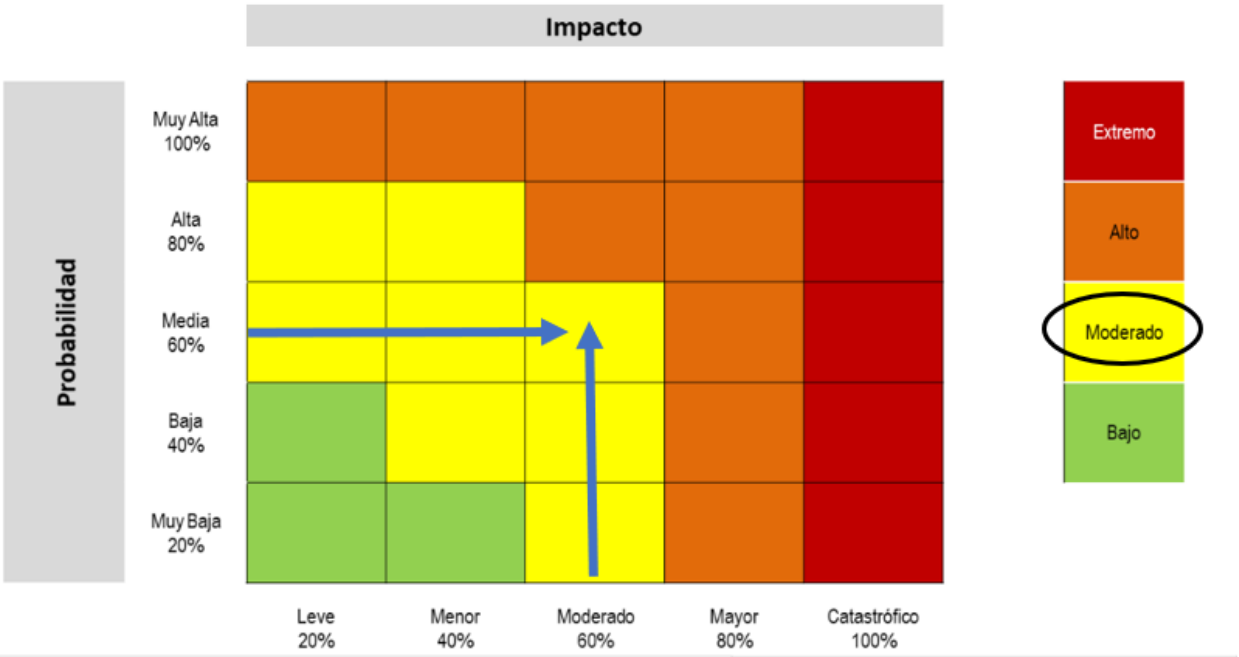
  - "*Con registro manual*: *El control deja un registro que permite evidenciar la ejecución del control*".[9]

- La ejecución del control es interna: "es decir que la Entidad cuenta con formatos o registros internos formales."[10]

La matriz de calor para este control es la siguiente:

[7] Ídem al anterior
[8] Ídem al anterior
[9] ídem al anterior
[10] Ídem al anterior

Ilustración 2 Matriz inherente de calor - nivel de severidad



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 7 - agosto de 2025.
Elaboró: Profesional de la Oficina de Evaluación y Control

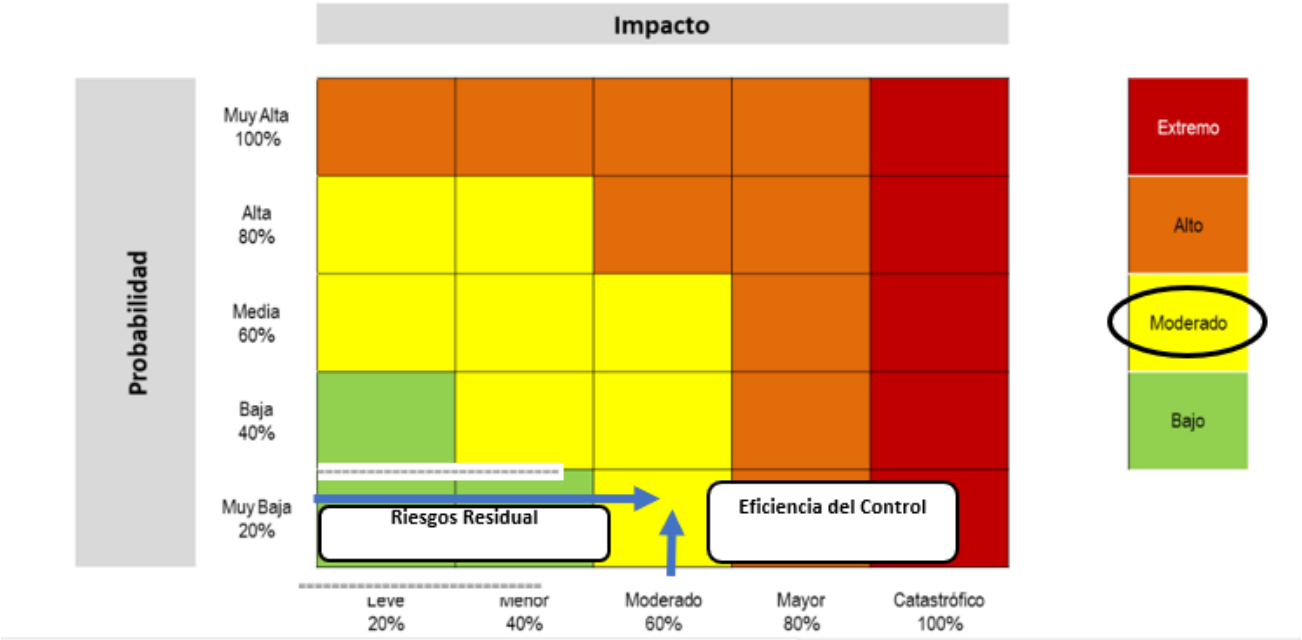
La probabilidad de ocurrencia es media y el impacto moderado, lo ubica en la matriz de calor de severidad moderado, como se detalla en la ilustración No. 2.

Con la valoración de los controles se obtiene:

- Probabilidad Residual: Baja 36%
- Impacto Residual: Moderado 60%
- Zona de riesgo residual: Moderado

Tal como se muestra en la siguiente ilustración:

Ilustración 3 Matriz de calor residual – nivel de severidad de los controles identificados



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 7 - agosto de 2025.
Elaboró: Profesional de la Oficina de Evaluación y Control

La probabilidad de ocurrencia es muy baja y el impacto moderado, lo ubica en la matriz de calor de severidad moderado, como se detalla en la ilustración No. 5 Matriz de calor residual – nivel de severidad de los controles identificados.

Tabla 5 Nivel del riesgo identificado después de valorar los controles

INHERENTE	CONTROLES	RESIDUAL	ANÁLISIS
MODERADO	1	MODERADO	Se desplaza en probabilidad Baja la probabilidad, continúa en la zona MODERADA

Elaboró: Profesional de la Oficina de Evaluación y Control

10. CONCLUSIONES

- ✓ La auditoría evidencia que la Institución dispone de una base documental para la gestión de seguridad y privacidad de la información, conformada por planes, manuales y procedimientos que cubren componentes relevantes del MSPI, entre ellos riesgos, respaldos, accesos e incidentes. También se identifican avances frente a la formalización de la gestión de incidentes y al seguimiento de riesgos.

- ✓ El nuevo soporte permite corregir las afirmaciones preliminares sobre documentación no aportada, pero no acredita por sí mismo la clasificación integral de activos de información, una Declaración de Aplicabilidad individualizada, pruebas técnicas satisfactorias de restauración o recuperación, ni la ejecución y cobertura de capacitaciones específicas en 2026. Estas materias permanecen como oportunidades de fortalecimiento de trazabilidad y evidencia, no como incumplimientos materiales automáticamente demostrados.

- ✓ En consecuencia, la valoración final es favorable respecto de la formalización y de la respuesta documental complementaria, con oportunidades de mejora para demostrar la ejecución y efectividad de los controles. Las tres situaciones del preinforme se reformulan a la luz de los nuevos soportes; ninguna debe conservar una afirmación de ausencia documental que haya quedado desvirtuada.

- ✓ Respecto de los indicadores, la situación identificada en la auditoría anterior se mantiene bajo seguimiento a través del Plan de Mejoramiento N.°063, razón por la cual no se formula una observación adicional sobre el mismo hecho.

11. RECOMENDACIONES

Con fundamento en los resultados obtenidos durante la auditoría, la Oficina de Evaluación y Control presenta las siguientes recomendaciones, orientadas al fortalecimiento continuo del Modelo de Seguridad y Privacidad de la Información MSPI:

- ✓ Vincular el inventario recibido con un registro específico de activos de información y su clasificación, responsables, riesgos y controles; conservar disponible la Declaración de Aplicabilidad y la medición de línea base del MSPI, si existen, o definir su formalización y seguimiento.

- ✓ Establecer una correspondencia verificable entre el inventario patrimonial o tecnológico y el inventario de activos de información, evitando tratarlos como instrumentos equivalentes.

- ✓ Mantener un diagnóstico o línea base del MSPI que permita medir periódicamente el avance, las brechas y las prioridades de mejora.

- ✓ Fortalecer la gestión de continuidad y recuperación mediante pruebas periódicas documentadas, seguimiento a resultados y acciones de mejora.

- ✓ Conservar evidencia de actividades de sensibilización efectivamente ejecutadas, con contenidos, fecha, población objetivo, asistencia, cobertura y evaluación de apropiación cuando corresponda.

- ✓ Continuar el seguimiento al Plan de Mejoramiento N.°063 y evitar el cierre de acciones únicamente por existencia documental, privilegiando evidencia de operación y resultados.

- ✓ Fortalecer la conservación y disponibilidad de evidencias de ejecución de controles, de manera que permitan valorar su diseño, operación y efectividad.

- ✓ Se recomienda formular e implementar plan de mejoramiento que incorpore los hallazgos y oportunidades de mejora identificadas en el presente informe de auditoría, definiendo acciones, responsables, plazos y mecanismos de seguimiento.

12. GLOSARIO

Auditoría Interna: Proceso sistemático, independiente y documentado mediante el cual se obtiene y evalúa objetivamente evidencia para determinar el grado de cumplimiento de los criterios establecidos y formular recomendaciones orientadas al mejoramiento continuo.

MSPI: Modelo de Seguridad y Privacidad de la Información.

SoA: Statement of Applicability o Declaración de Aplicabilidad; instrumento que permite documentar la selección, aplicación y justificación de controles de seguridad.

DRP: Disaster Recovery Plan o Plan de Recuperación ante Desastres.

Activo de información: Información, sistema, servicio, recurso tecnológico u otro elemento que posee valor para la organización y requiere protección.

13. ANEXOS

No se presentaron Anexos.

14. BIBLIOGRAFÍA

- ✓ Departamento Administrativo de la Función Pública – DAFP. (2023). Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 7.
- ✓ Ley 87 de 1993.
- ✓ Resolución MinTIC 00500 de 2021 y Anexo 1 – Modelo de Seguridad y Privacidad de la Información.
- ✓ Informe de Auditoría MSPI vigencia 2025 – Oficina de Evaluación y Control.
- ✓ Plan de Seguridad y Privacidad de la Información – GT-MA-006.
- ✓ Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – GT-MA-004.

- ✓ Manual para realizar backups y recuperación de desastres informáticos – GT-MA-002.
- ✓ Procedimiento Gestión de Incidentes de Seguridad Digital – GT-PR-014.
- ✓ Documentación y evidencias suministradas por Gestión de Tecnología y Medios Audiovisuales durante la auditoría 2026.

Andersson Benitez A

Elaboró: **Andersson Benítez Arboleda**
Profesional Oficina Evaluación y Control
Fecha: 15 de octubre 2026

Carlos Alberto Toro M

Revisó y Aprobó: **Carlos Alberto Toro Mejía**
Jefe Oficina Evaluación y Control
Fecha: 15 de octubre 2026