



MEMORANDO
1400

FECHA: Medellín, 30 de diciembre de 2022

PARA:
JUAN DAVID GOMEZ FLOREZ
RECTOR DE INSTITUCIÓN UNIVERSITARIA
RECTORÍA

DE:
JUAN DAVID CALLE TOBON
DIRECTOR(A) OPERATIVO

ASUNTO: Remisión informe definitivo auditoría legal Modelo de Seguridad y Provacidad de la Información

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 sesión ordinaria del 09 de diciembre de 2021 y modificado y aprobado en sesión extraordinaria del 08 de julio de 2022, me permito hacer entrega del informe definitivo correspondiente a la auditoría de ley que se practicó por parte de la Oficina de Evaluación y Control de la Institución al Modelo de Seguridad y Privacidad de la Información.

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 resultados obtenidos con los responsables de la unidad auditable al interior de la Institución, por tanto, son conocedores de las oportunidades de mejora identificadas.





Finalmente, y en aras de la mejora continua de la Institución, de forma respetuosa, le informo que la Institución dispone de cinco (5) días hábiles para presentar el plan de mejoramiento, en el que se establezcan las acciones a que haya lugar a fin de subsanar las deficiencias evidenciadas

Atentamente,

JUAN DAVID CALLE TOBON
DIRECTOR(A) OPERATIVO
OFICINA DE EVALUACIÓN Y CONTROL

Anexos: (19)folios



INFORME DE AUDITORÍA

CONTROL INTERNO



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

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

INFORME
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)
VIGENCIA 2022

Equipo de trabajo

JUAN DAVID CALLE TOBÓN
Director Oficina Evaluación y Control

PAULINA RÍOS ARCE
Profesional Oficina Evaluación y Control

Oficina de Evaluación y Control
Diciembre 2022

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

Contenido

PRESENTACIÓN	5
1. ALCANCE DE LA AUDITORÍA	6
2. RIESGOS ASOCIADOS A LA UNIDAD AUDITABLE	6
3. CRITERIOS DE AUDITORÍA	7
4. OBJETIVOS	7
4.1 OBJETIVO GENERAL	7
4.2 OBJETIVOS ESPECÍFICOS	7
5. METODOLOGÍA	8
6. LIMITACIONES	8
7. MUESTRA	8
8. RESUMEN	9
9. RESULTADOS DE LA AUDITORÍA	10
9.1 HALLAZGOS	10
10. CONCLUSIONES	18
11. RECOMENDACIONES	18
12. BIBLIOGRAFÍA	19

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín

Distrito de
Ciencia, Tecnología e Innovación

Lista de tablas

Tabla 1.....	6
Tabla 2.....	7
Tabla 3.....	11
Tabla 4.....	13
Tabla 5.....	16

Lista de ilustraciones

Ilustración 1	14
Ilustración 2	15
Ilustración 3	17

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
 Distrito de
 Ciencia, Tecnología e Innovación

PRESENTACIÓN

Con fundamento en Ley 87 de 1993, en la Resolución No. 089 del 29 de abril del 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 sesión ordinaria del 09 de diciembre de 2021 y modificado y aprobado en sesión extraordinaria del 08 de julio de 2022, la Oficina de Evaluación y Control realizó auditoría legal al Modelo de seguridad y Privacidad de la Información.

La actividad de auditoría interna de la Institución Universitaria Colegio Mayor de Antioquia, es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la entidad. Ayuda a la Institución a cumplir sus objetivos, aportando un enfoque sistemático y disciplinario para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, controles y gobierno, a través de servicios de aseguramiento y consultoría.

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, a partir de esta auditoría es importante se establezcan las acciones, los métodos, procedimientos y mecanismos de prevención, corrección, evaluación y de mejoramiento continuo del proceso, a que haya lugar, con el fin de garantizar el cumplimiento de las disposiciones legales inherentes en la materia.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín

Distrito de
Ciencia, Tecnología e Innovación

1. ALCANCE DE LA AUDITORÍA

La auditoría considerará la verificación de la implementación de las 5 fases del modelo:

- I. Diagnóstico.
- II. Planificación.
- III. Operación.
- IV. Evaluación de desempeño.
- V. Mejoramiento continuo.

2. RIESGOS ASOCIADOS A LA UNIDAD AUDITABLE

Tabla 1

Tipo de Riesgo	Escenario de riesgo	Observación
Incumplimiento	No acatar las disposiciones y los requerimientos legales vigentes en lo inherente al seguimiento de los compromisos adquiridos en cada una de las instancias de la Institución como resultado de las reuniones ordinarias o extraordinarias realizadas.	No se evidenció la materialización de este riesgo para el periodo evaluado.
Corrupción	“Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado” ¹ .	No se evidenció la materialización de este riesgo para el periodo evaluado.
Fraude	Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio. ²	No se evidenció la materialización de este riesgo para el periodo evaluado.

¹ https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

² <https://iaia.org.ar/auditor-interno/glosario/>

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

3. CRITERIOS DE AUDITORÍA

Tabla 2

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.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

5. METODOLOGÍA

- Conocimiento unidad auditable
- Revisión normatividad
- Solicitar y verificar información
- Revisión acciones plan de mejoramiento vigencia anterior
- Comunicación de resultados.

6. LIMITACIONES

No se presentaron limitación durante el desarrollo de la auditoría.

7. MUESTRA

No se aplicó muestreo para la presente auditoría.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

8. RESUMEN

Se procedió a verificar el estado en que se encuentra la aplicación del Modelo de Privacidad y Seguridad de la Información en la Institución Colegio Mayor de Antioquia, modelo desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en el anexo 1 de la Resolución 00500 del 10 de marzo de 2021, en la presente auditoría se revisó el estado de las 5 fases que el modelo establece para su implementación.

Encontrándose que se ha cumplido con la fase I – Diagnostico, se encuentra culminando la fase II Planificación, para continuar con las siguientes: III- Operación, IV Evaluación de Desempeño y V Mejoramiento continuo.

Se evidenciaron aspectos de mejora como la elaboración e implementación del plan de capacitación, sensibilización y comunicación de seguridad de la información. Así como, la necesidad de la identificación de riesgos de seguridad y privacidad de la información con sus respectivos controles.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín

Distrito de
Ciencia, Tecnología e Innovación

9. RESULTADOS DE LA AUDITORÍA

9.1 HALLAZGOS

Por medio de la resolución 00500 de 2021 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información, como habilitador de la Política de Gobierno Digital. Esta norma tiene por objeto establecer los lineamientos para la implementación del modelo.

Los sujetos obligados son las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998, es decir, los órganos que conforman la rama ejecutiva del poder público y los demás organismos y entidades de naturaleza pública que de manera permanente tengan a su cargo el ejercicio de actividades y funciones administrativas o la prestación de servicios públicos.

Acorde con lo anterior, los sujetos obligados deben adoptar medidas técnicas, administrativas y del talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información, y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías manuales y formatos para garantizar el cumplimiento del ciclo PHVA del Modelo de Seguridad y Privacidad de la Información, por lo tanto, deben adoptar los lineamientos del modelo que se relacionan en el anexo 1 de la resolución 00500 de 2021.³

Con el fin de realizar el seguimiento a la implementación del MSPI por parte de la Institución Colegio Mayor de Antioquia, se procedió a verificar la ejecución de las 5 fases del modelo, las cuales permiten según la normativa, gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información:

- I. Diagnóstico.
- II. Planificación.
- III. Operación.
- IV. Evaluación de desempeño.
- V. Mejoramiento continuo.

³ Artículo 3 resolución 00500 de 2021.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
 Distrito de
 Ciencia, Tecnología e Innovación

Evidenciándose lo siguiente:

- I. Diagnóstico: su objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI.

Se aportó lo siguiente: Instrumento de identificación de la línea base de seguridad.

- II. Planificación: Determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta el mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Se evidencia que la Institución cuenta con el Plan de Seguridad y Privacidad de Información que se encuentra en formato GT-MA-006 del 1 de febrero de 2022.

Los documentos que se generan en esta fase son los siguientes:

Tabla 3

Documento	Evidencia
Alcance MSPI	Archivo Instrumento de identificación de la línea base de seguridad.
Acto administrativo con las funciones de seguridad y privacidad de la Información	Resolución 087 de 2018 , a través del cual se crean o se modifican las funciones del comité institucional de desarrollo administrativo o el que haga sus veces, donde se incluyen los temas de seguridad y privacidad de la información.
Política de seguridad y privacidad de la información	Acuerdo 09 de 2018 , por medio del cual se adopta la Política de Seguridad y Privacidad de la Información de la Institución.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
 Distrito de
 Ciencia, Tecnología e Innovación

Documentos de roles y responsabilidades asociadas a la seguridad y privacidad de la información.	Archivo Instrumento de identificación de la línea base de seguridad en las pestañas áreas involucradas y administrativas.
Procedimiento de inventario y Clasificación de la Información e infraestructura crítica	Plan Estratégico de Tecnología de la Información y las Comunicaciones PETIC 2021-2023, GT-MA-005.
Metodología de inventario y clasificación de la información e infraestructura crítica	Plan Estratégico de Tecnología de la Información y las Comunicaciones PETIC 2021-2023, GT-MA-005.
Procedimiento de gestión de riesgos de seguridad de la información	Plan de tratamiento de riesgos de seguridad y privacidad de la información- GR-MA-004.
Plan de tratamiento de riesgos de seguridad de la información	Plan de tratamiento de riesgos de seguridad y privacidad de la información- GR-MA-004.
Declaración de aplicabilidad	Plan de tratamiento de riesgos de seguridad y privacidad de la información- GR-MA-004.
Manual de políticas de Seguridad de la Información	Acuerdo 09 de 2018 , por medio del cual se adopta la Política de Seguridad y Privacidad de la Información de la Institución.
Plan de capacitación, sensibilización y comunicación de seguridad de la información	Se encuentra pendiente de desarrollo pues se esta en la etapa de apropiación digital. En la presente vigencia se envió encuesta.

- III. Operación: Consiste en Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Los documentos que se deben generar en esta fase son:

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

Tabla 4

Documento	Evidencia
Plan de implementación de controles de seguridad y privacidad de la información	Plan de tratamiento de riesgos de seguridad y privacidad de la información- GR-MA-004.
Evidencia de la implementación de los controles de seguridad y privacidad de la información.	No se identifican riesgos de seguridad de la información como pérdida de confiabilidad, integridad y disponibilidad, y de sus controles en el mapa de riesgos institucional

- IV. Evaluación de desempeño: Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.⁴
- V. Mejoramiento continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

La Institución Universitaria Colegio Mayor de Antioquia, se encuentra en la fase de “planeación”, la cual puede durar 1 año y medio o dos años, por lo tanto, aún no se ha llegado a la etapa de evaluación del desempeño y la etapa subsiguiente mejoramiento continuo.

9.1.2. Observaciones

9.1.2.1. Plan de capacitación y comunicación de seguridad de la información.

El artículo 5 de la resolución 00500 de 2021 de MINTIC, establece:

(...) La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la

⁴ Anexo 1 Modelo de seguridad y Privacidad de la Información.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

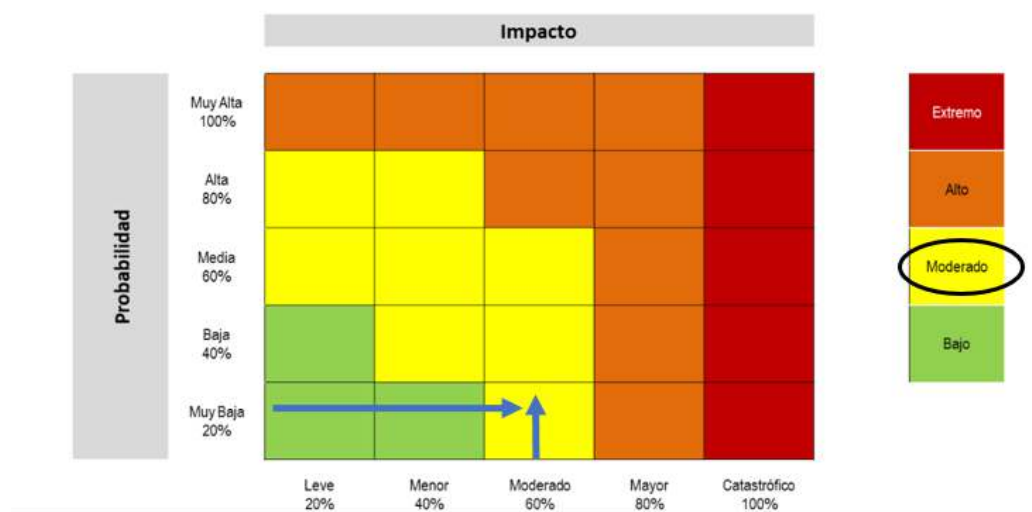
4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.”

Durante la ejecución de la auditoría no se evidenció la realización del plan de capacitación, sensibilización y comunicación de seguridad de la información en la Institución.

Riesgo identificado:

- Riesgo de cumplimiento: incumplimiento de las disposiciones normativas.

Ilustración 1



NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín

Distrito de
Ciencia, Tecnología e Innovación

La probabilidad de ocurrencia del riesgo es muy baja y el impacto es moderado lo que lo ubica en la matriz de calor en un riesgo moderado.

9.1.2.2. Controles de riesgos de Seguridad y Privacidad de la información.

El artículo 6 de la resolución 00500 de 2021, señala:

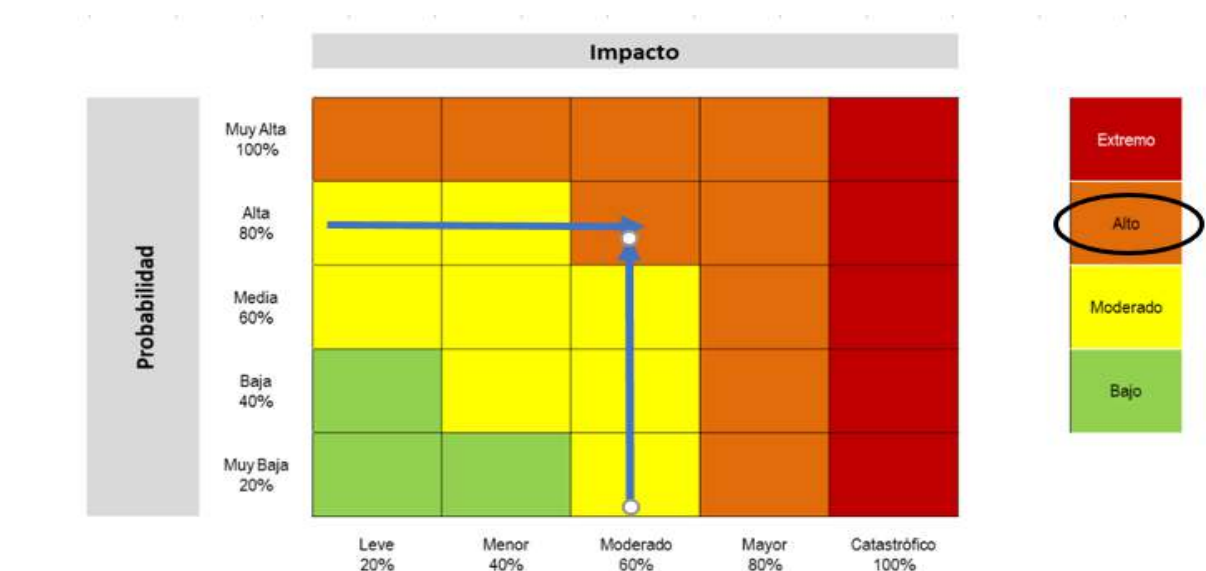
“La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades (...).”

No se identifica en el mapa de gestión de riesgos de la institución, riesgos de seguridad de la información como: pérdida de confiabilidad, integridad y disponibilidad ni de sus controles.

Riesgo identificado:

- Riesgo de seguridad de la información: pérdida de la confidencialidad, integridad y disponibilidad de la información institucional.

Ilustración 2



NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

La probabilidad de ocurrencia del riesgo es alta y el impacto es moderado lo que lo ubica en la matriz de calor en un riesgo alto.

9.2. EVALUACIÓN DE CONTROLES

Conforme la “Guía para la administración del riesgo y diseño de controles en entidades públicas” versión 5, de diciembre de 2020, expedida por el Departamento Administrativo de la Función Pública, se verificaron los controles establecidos por la institución.

De conformidad con la guía, un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta lo siguiente:

- Identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

En el mapa de Riesgos de Gestión -2021 de la Institución, se identifica el siguiente control: *“El líder de Tecnología verifica el cumplimiento de la política de seguridad de la información por parte de los usuarios y realiza periódicamente campañas para que los usuarios trabajen en la unidad de red de la cual se hace copia de respaldo con periodicidad diaria o en su defecto salvaguarden la información en el drive donde se garantiza copia permanente ya sea en google drive o en Microsoft one drive.”*. Al realizar la evaluación del punto de control se identificó:

Tabla 5

Control	Características				Peso
Control: El líder de Tecnología verifica el cumplimiento de la política de seguridad de la información por parte de los usuarios y realiza periódicamente	Atributos de Eficiencia	Tipo	Preventivo	x	25%
			Detectivo		0%
			Correctivo	X	10%
	*Atributos de Formalización	Implementación	Automático		0%
			Manual	X	15%
		Documentación	Documentado	X	si
			Sin Documentar		—

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



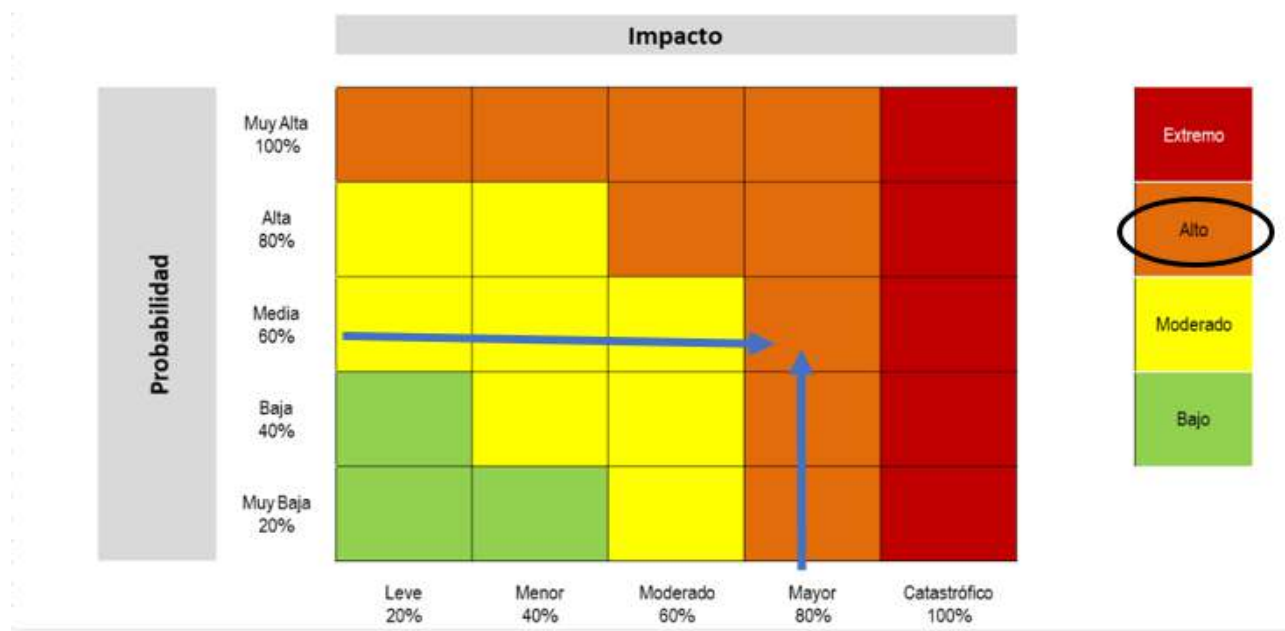
Alcaldía de Medellín

Distrito de
Ciencia, Tecnología e Innovación

campañas para que los usuarios trabajen en la unidad de red de la cual se hace copia de respaldo con periodicidad diaria o en su defecto salvaguarden la información en el drive donde se garantiza copia permanente ya sea en google drive o en Microsoft one driven.		Frecuencia	Continua	X	si
			Aleatoria		—
		Evidencia	Con Registro	X	si
			Sin Registro		—
Total valoración del control					40%

Para este control la probabilidad de ocurrencia es media y el impacto es mayor, lo que lo ubica en la matriz de calor en un riesgo alto:

Ilustración 3



NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
 Distrito de
 Ciencia, Tecnología e Innovación

10. CONCLUSIONES

- La institución se encuentra adoptando de forma adecuada el Modelo de Seguridad y Privacidad de la Información, con el fin de mitigar los riesgos relacionados a la protección y privacidad de la información e incidentes de seguridad digital, encontrándose en la fase II “Planificación”.
- Se cuenta con un grupo de trabajo encargado de implementar el Modelo de Seguridad de la Información, conformado por los funcionarios del área de Tecnología y Medios Audiovisuales de la institución y un asesor de Gobierno Digital.
- La institución debe continuar aunando sus esfuerzos para culminar de manera satisfactoria la fase de planificación y continuar con las etapas subsiguientes, con el fin de implementar de manera completa el Modelo de Seguridad y Privacidad de la Información.

11. RECOMENDACIONES

- Generar un cronograma de implementación del Modelo de Seguridad y Privacidad de la información, teniendo en cuenta las 5 fases establecidas en el anexo 1 de la Resolución 00500 de 2021.
- Desarrollar en la vigencia 2023 el Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información para implementarlo de forma anual en la institución.
- Identificar en conjunto con el área de planeación los riesgos de seguridad de la información tales como: pérdida de la confidencialidad, integridad y disponibilidad y como consecuencia establecer los controles respectivos e incluirlos en el Mapa de Gestión de Riesgos Institucional.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín

Distrito de
Ciencia, Tecnología e Innovación

12. BIBLIOGRAFÍA

- Resolución 00500 de 2021.
- Decreto 1078 de 2015.
- Acuerdo 09 de 2018.
- Decreto 2106 de 2019.

Elaboró:



Paulina Ríos Arce – Profesional Oficina Evaluación y Control
Fecha: 29 de diciembre de 2022

Revisó y Aprobó:



Juan David Calle Tobón – Jefe Oficina Evaluación y Control
Fecha: de diciembre de 2022.

NIT: 890980134-1



WWW.COLMAYOR.EDU.CO



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación