INFORME DE AUDITORÍA											
Proceso:	**Gestión de Servicios TIC**										
Numero de Auditoria:	**2020-AE-04** **AUDITORIA INTERNA COMBINADA DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA NTC ISO/IEC 27001:2013**										
Reunión de Apertura						**Reunión de Cierre**					
Día	08	**Mes**	06	**Año**	2020	**Día**	14	**Mes**	08	**Año**	2020

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S): Roger Quirama García-Jefe Oficina de Tecnología y Sistema de la Información.

EQUIPO AUDITOR

AUDITOR LIDER ISO/IEC 27001:2013: Clara Patricia Muñoz Jiménez

OBJETIVO DE AUDITORÍA:

Evaluar el Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información, en su alcance correspondiente al proceso de Gestión de Servicios TIC del Ministerio de Educación Nacional – MEN, conforme a los requisitos legales vigentes de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - MIN TIC y la norma NTC ISO/IEC 27001:2013.

ALCANCE DE AUDITORÍA:

El alcance se definió para el Sistema de Gestión de Seguridad de la Información relacionado con el proceso de Gestión TIC del Ministerio de Educación Nacional - MEN, correspondiente a la vigencia 2019 y hasta el 31 de mayo de 2020.

CRITERIOS DE AUDITORÍA:

- Auditoría interna con base en norma NTC-ISO-IEC 27001:2013
- Decreto 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
- Documentación interna (procesos, procedimiento, políticas, directrices, etc.) del Sistema de Gestión Integrado del Ministerio de Educación Nacional.

METODOLOGÍA:

Técnicas de auditoría basadas en los métodos de observación, confrontación, revisión y comparación. De acuerdo con las mejores prácticas de auditoria se verificará el cumplimiento del sistema de gestión, procedimientos, registros, instructivos y demás documentos que soporten el modelo referencial.

SESIONES DE AUDITORÍA:

SGSI-01: junio 08 de 2020. 08:30 a.m. a 10:00 a.m. Requisito 4. Contexto de la Entidad.
SGSI-02: junio 08 de 2020. 10:30 a.m. a 12:30 p.m. Requisito 5. Liderazgo.
SGSI-03: junio 09 de 2020. 08:00 a.m. a 10:00 a.m. Requisito 6. Planeación.
SGSI-04: junio 09 de 2020. 10:30 a.m. a 12:30 p.m. Requisito 8. Operación y Controles A.8 Gestión de Activos
SGSI-05: junio 10 de 2020. 08:00 a.m. a 10:00 a.m. Requisito 7. Soporte y Controles A.7 Recursos Humanos
SGSI-06: junio 10 de 2020. 10:30 a.m. a 12:30 p.m. Controles A.9 Gestión de Acceso
SGSI-07: junio 11 de 2020. 08:00 a.m. a 10:00 a.m. Controles A.11 Seguridad Física y Ambiental
SGSI-08: junio 11 de 2020. 10:30 a.m. a 12:30 p.m. Controles A.12 Seguridad en Operaciones
SGSI-09: junio 12 de 2020. 08:00 a.m. a 10:00 a.m. Controles A.13 Seguridad en Comunicaciones

SGSI-10: junio 12 de 2020. 10:30 a.m. a 12:30 p.m. Controles A.14 Adquisición, Desarrollo y Mantenimiento SW
SGSI-11: junio 16 de 2020. 08:00 a.m. a 10:00 a.m. Controles A.15 Relaciones con Proveedores
SGSI-12: junio 16 de 2020. 10:30 a.m. a 12:30 p.m. Controles A.16 Gestión de Incidentes de Seguridad Información
SGSI-13: junio 17 de 2020. 08:00 a.m. a 10:00 a.m. Controles A.17 Seguridad en la Gestión de Continuidad Negocio
SGSI-14: junio 17 de 2020. 10:30 a.m. a 12:30 p.m. Requisito 9. Evaluación Desempeño. Controles A.18 Cumplimiento
SGSI-15: junio 18 de 2020. 08:00 a.m. a 09:30 a.m. Requisito 9. Supervisión, Medición y Evaluación
SGSI-16: junio 18 de 2020. 10:00 a.m. a 11:30 a.m. Requisito 9. Revisión por la Dirección
SGSI-17: junio 18 de 2020. 11:30 a.m. a 12:30 p.m. Requisito 10. Mejora

1. RESUMEN GENERAL

Se destaca la buena disposición para la atención de la auditoría interna combinada remota por parte de las áreas y funcionarios auditados, y el apoyo logístico de la Subdirección de Desarrollo Organizacional, la Oficina de Control Interno y la Oficina de Tecnología y Sistemas de Información.

A continuación, un resumen de los resultados de la ejecución del plan de auditoría interna al Sistema de Gestión de Seguridad de la Información – SGSI, del Proceso de Gestión de Servicios TIC del Ministerio de Educación Nacional, bajo la norma NTC/ISO 27001:2013, realizada en 17 sesiones virtuales programadas por la plataforma de TEAMS del MEN, durante el periodo comprendido entre el 8 y 18 de junio de 2020:

ITEM	RESULTADO GENERAL	CANTIDAD
1	FORTALEZAS	36
2	OPORTUNIDADES DE MEJORA – REQUISITOS DE NORMA	7
3	OPORTUNIDADES DE MEJORA – OBJETIVOS DE CONTROL	10
	TOTAL	**53**

Se revisaron 130 requerimientos de Norma NTC/ISO 27001:2013 repartidos en 7 numerales, y 114 controles del Anexo A correspondientes a 14 dominios de control. La auditoría se realizó con la participación de auditados de las áreas: Oficina de Tecnología y Sistemas de Información, Subdirección de Desarrollo Organizacional, Oficina de Control Interno, Subdirección de Acceso, Subdirección de Desarrollo Sectorial, Subdirección de Contratación, Subdirección de Gestión Administrativa, Subdirección de Talento Humano, Oficina Asesora de Comunicaciones y Dirección de Cobertura y Equidad.

2. RESULTADOS DE AUDITORIA

2.1 Sesión de Auditoría SGSI-01

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Numeral 4. Contexto de la Entidad.

Criterios de Auditoría:

Requisitos de Norma: 4.1 Entendiendo la entidad y su contexto; 4.2 Entendiendo las necesidades y expectativas de las partes interesadas; 4.3 Determinando el alcance del sistema de gestión de seguridad y, 4.4 Estableciendo el Sistema de Gestión de la Seguridad de la Información.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
PLANEAR	4	CONTEXTO DE LA ENTIDAD				
	4.1	Entendiendo la entidad y su contexto	X			
	4.2	Entendiendo las necesidades y expectativas de las partes interesadas	X			X
	4.3	Determinando el alcance del sistema de gestión de seguridad	X			X
	4.4	Sistema de Gestión de la Seguridad de la Información.	X			

Fortalezas:

- El Ministerio tiene determinado el contexto al que se enfrenta el sector educativo, pieza fundamental para mitigar los aspectos externos e internos que pueden afectar el adecuado direccionamiento del sector y poner en riesgo el cumplimiento de los objetivos estratégicos, así como el logro del propósito superior planteado para la educación colombiana. Es así como el MEN considera los aspectos fundamentales que deben ser tenidos en cuenta en el sector, en el Ministerio y en la operación del Sistema Integrado de Gestión - SIG, en el marco de lo planteado en el Modelo Integrado de Planeación y Gestión – MIPG; específicamente, con el modelo referencial del sistema de gestión de seguridad de la información.

- Para facilitar la identificación de todas las partes interesadas o grupos del valor, el Ministerio desarrolló la Guía Metodológica para la Caracterización de Partes Interesadas, con el objetivo de dar orientaciones en el diseño y aplicación de ejercicios de caracterización de grupos de valor, ciudadanos, usuarios e interesados, y en el uso de los resultados de dichos ejercicios.

- El MEN a través de la resolución 17564 de 2019, definió que el SGSI recoge los lineamientos del Ministerio de las TIC para el desarrollo de seguridad digital de MIPG, buscando gestionar adecuadamente la seguridad y privacidad de los activos de información, en el marco de la estrategia de Gobierno Digital, establecido en el Decreto 1078 de 2015.

Oportunidades de Mejora:

- **OM01.** En la identificación las partes interesadas, con base en la aplicación de la metodología, se delimitaron 27 grupos de valor en el ecosistema sectorial, agrupados en 18 categorías. No obstante considerar la seguridad de la información como un elemento transversal, los requisitos de las partes interesadas se deben determinar claramente en el Sistema de Gestión de Seguridad de la Información. (Numeral 4.2.b.)

- **OM02.** Se deben precisar claramente los límites y aplicabilidad del Sistema de Gestión de Seguridad de la Información para establecer el alcance, teniendo en cuenta las interfaces y dependencias entre las actividades realizadas por el MEN y aquellas que son realizadas por otras Entidades y Organizaciones. En general, se trata de un documento independiente, aunque puede ser unificado con una política de seguridad de la información. (Numeral 4.3.c).

2.2 Sesión de Auditoría SGSI-02

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Numeral 5. Liderazgo.

Criterios de Auditoría:
Requisitos de Norma: 5.1 Liderazgo y compromiso; 5.2 Política y 5.3 Roles, responsabilidades y autoridades en la entidad. Objetivos de control: A.5. Políticas de seguridad de la información y A.6 Organización de la seguridad de la información.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
PLANEAR	5	LIDERAZGO				
	5.1	Liderazgo y compromiso	X			
	5.2	Política	X			X
	5.3	Roles, responsabilidades y autoridades en la entidad.	X			
	A.5	Políticas de seguridad de la información	X			X
	A.6	Organización de la seguridad de la información	X			

Fortalezas:

- Según la Resolución 1760 de 2018 en el art.3, el SIG del MEN está compuesto por los modelos referenciales: Sistema de Gestión de la Calidad, Sistema de Gestión de Seguridad de la Información, Sistema de Gestión de Seguridad y Salud en el Trabajo, Sistema de Gestión Ambiental y Modelo Estándar de Control Interno, como herramienta transversal de seguimiento y control. En el art. 5 se describe la Política de Seguridad de la Información: *"Seguridad de la Información: identificar, gestionar y reducir los riesgos a los cuales se expone la información, asegurando la confidencialidad, integridad y disponibilidad de la misma en la entidad, así como la continuidad de las operaciones del MEN y la consolidación de una cultura de seguridad que permita el cumplimiento de los requisitos legales y contractuales vigentes"*.

- Según la Resolución 17564 de 2019, en el art. 6, a través del Comité de Dirección y el Comité Institucional de Gestión y Desempeño se informa trimestralmente sobre el desempeño del SGSI y sus acciones de mejora. Según acta de marzo de 2019, se revisa la formulación del Plan de acción institucional y los planes estratégicos de MIPG, y se socializan los resultados del reporte realizado en FURAG y del EDI. (Acta Comité 26 marzo-2019 - PM-FT-01 v3).

- Según la misma Resolución 17564 de 2019, en el art. 8, se describe el mapa de procesos, la cadena de valor del Ministerio compuesta por 6 procesos estratégicos, 4 procesos misionales, 6 procesos de apoyo y un proceso de evaluación y control. Se resalta que el Proceso de Gestión de Servicios TIC fue migrado del grupo de Procesos de Soporte al grupo de Procesos Estratégicos, donde se gestiona el Sistema de Gestión de Seguridad de la Información- SGSI.

Oportunidades de Mejora:

- **OM03.** Según el Manual de Seguridad Informática, ST-MA-02 v3, el objetivo es propender porque los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad, brindando un nivel de seguridad óptimo, y que permitan: disminuir las amenazas a la seguridad de la información y los datos, evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos, cuidar y proteger los recursos tecnológicos del MEN y concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación. Por lo dicho, es requerido que se definan de forma clara los objetivos y metas de la seguridad de la información, alineados con los objetivos del Sistema Integrado de Gestión – SIG y los objetivos estratégicos del Ministerio de Educación Nacional. (Numeral 5.2.b.)

- **OM04.** En el Manual de Políticas de Seguridad de la Información PM-MA-03 v3, se tienen definidas 22 Políticas del SGSI, a las cuales se les está dando el enfoque de presentación como guías de políticas de seguridad de la información, facilitando su divulgación, entendimiento y concientización por cada una de las partes interesadas del SGSI. Es necesario agilizar su desarrollo, aprobación y divulgación para facilitar la concientización de las partes interesadas en las políticas específicas del Sistema de Gestión de Seguridad de la Información. (Objetivo de Control A.5.2).

2.3 Sesión de Auditoría SGSI-03

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Numeral 6. Planeación.

Criterios de Auditoría:
Requisitos de Norma: 6.1 Acciones para abordar los riesgos y las oportunidades; 6.2 Objetivos de seguridad de la información y planificación para lograrlos.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
PLANEAR	6	PLANEACIÓN	X			
	6.1	Acciones para abordar los riesgos y las oportunidades.	X			X
	6.2	Objetivos de seguridad de la información y planificación para lograrlos.	X			X

Fortalezas:

- El Ministerio aplica como herramienta de gestión de riesgos la metodología basada en la *"Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Riesgos de Gestión, Corrupción y Seguridad Digital. V4"*, de la Función Pública 2018, la cual fortalece la gestión preventiva encaminada al adecuado tratamiento de los riesgos institucionales, de calidad, seguridad y privacidad en la información, ambientales y de seguridad y salud en el trabajo, identificados en cada uno de los procesos que hacen parte del Sistema Integrado de Gestión.

- Para los riesgos institucionales, de procesos y del SGSI, SGSST y SGA, las frecuencias de seguimiento y reporte de avances en el plan de tratamiento, por parte de los líderes y responsables de proceso no superar los tres meses, de forma que permitan que el autocontrol realizado sea la base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.

- Para gestionar el riesgo en el SGSI, se identifican las amenazas potenciales para los activos de información, si existe algún riesgo que pueda afectar adversamente la confidencialidad, integridad o disponibilidad de la información. El tratamiento de los riesgos se realiza mediante una selección de controles tendientes a efectuar la reducción o mitigación de los riesgos encontrados.

Oportunidades de Mejora:

- **OM05.** El documento PM-FT-11 v03, contiene la Declaración de Aplicabilidad del SGSI del MEN, aprobada el 14 de marzo de 2019 y se registran los controles de seguridad que son aplicables (necesarios) y si éstos se encuentran operando o todavía no, las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso (Numeral 6.1.3.d.). En el documento PM-FT-11 v03, no se encuentra el control A.18.2.3 Revisión de cumplimiento técnico.
- **OM06.** En el documento PM-MA-01 v05, Manual del Sistema Integrado de Gestión, se tienen definido el objetivo general del SGSI: "identificar, gestionar y reducir los riesgos a los cuales se expone la información, asegurando la confidencialidad, integridad y disponibilidad de la misma en la entidad, así como la continuidad de las operaciones del MEN y la consolidación de una cultura de seguridad que permita el cumplimiento de los requisitos legales y contractuales vigentes". Sin embargo, para el desarrollo de las políticas específicas de seguridad de la información se requiere tener claramente sus objetivos de seguridad, los que se podrían clasificar en la protección de activos de información, autenticación, autorización e integridad de la información y auditoría de actividades de seguridad de la información (Numeral 6.3).

2.4 Sesión de Auditoría SGSI-04

Objetivo:

Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Numeral 8. Operación y Dominio de Control A.8 Gestión de Activos.

Criterios de Auditoría:

Requisitos de Norma: 8.1 Control y planificación operacional; 8.2 Evaluación de riesgo de la seguridad de la información; 8.3 Tratamiento de riesgo de la seguridad de la información. Objetivos de Control: A.8.1. Responsabilidad de los activos; A.8.2. Clasificación de la información y A.8.3. Manejo de medios.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	8	OPERACIÓN				
	8.1	Control y planificación operacional	X			
	8.2	Evaluación de riesgo de la seguridad de la información.	X			
	8.3	Tratamiento de riesgo de la seguridad de la información.	X			
	A.8	GESTIÓN DE ACTIVOS				
	A.8.1	Responsabilidad de los activos.	X			
	A.8.2	Clasificación de la información.	X			X
	A.8.3	Manejo de medios.	X			

Fortalezas:

- Dentro del SIG en el módulo del SGSI se tiene el inventario de activos de información, el cual se puede crear, actualizar, conservar, eliminar y tener el control de los activos de información de los procesos del MEN.

- Se realizan las evaluaciones de riesgos a intervalos planificados semestralmente aplicando la evaluación de riesgos de seguridad de la información. Se Identifican los activos de información determinando las salidas de información de esos activos. Se clasifican y se establece una prioridad sobre esa información. Se evalúa la prioridad de cada tipo de información mediante una puntuación o valoración del riesgo. Finalmente, se definen los controles necesarios para asegurar la información que supere determinado nivel de riesgo establecido, según los criterios de riesgo del Sistema de Gestión de Seguridad de la Información del Ministerio de Educación Nacional.

- La Oficina Tecnológica y Sistemas de Información cuenta con el contrato 1218 de 2018 del Proyecto Operación Global Servicios TICS con el Operador UNE EPM TELCO S.A., quién presenta mensualmente un informe de la gestión realizada a nivel de los servicios especializados de ejecución, administración y operación de seguridad informática del Ministerio de Educación Nacional de Colombia, en cuanto a planes de seguridad, gestión de vulnerabilidades operativas, disponibilidad de dispositivos de seguridad, gestión de identidad y acceso, cumplimiento del modelo operativo y planes de actualización tecnológica, entre otros.

Oportunidades de Mejora:

- **OM07.** Los activos de los sistemas que contienen información clasificada como sensible o crítica deberían llevar una etiqueta adecuada de clasificación. El etiquetado de la información clasificada es un requisito clave para los acuerdos que impliquen compartir información. El etiquetado afecta a la información y sus activos relacionados en formato físico y electrónico. Se debe realizar según el esquema de clasificación de la información. Las etiquetas deben reconocerse fácilmente. El etiquetado de la información puede realizarse de forma física o por medio de metadatos. (Objetivo de Control A.8.2).

2.5 Sesión de Auditoría SGSI-05

Objetivo:

Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Numeral 7. Soporte y Dominio de Control A.7 Seguridad de Recursos Humanos.

Criterios de Auditoría:

Requisitos de Norma: 7.1 Recursos; 7.2 Competencias; 7.3 Toma de conciencia; 7.4 Comunicación y 7.5 Información documentada. Objetivos de Control: A.7.2.2 Concientización, educación y formación en seguridad de la información.

CICLO DEL PROCESO	REQUISITO A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
PLANEAR	7	SOPORTE				
	7.1	Recursos.	X			
	7.2	Competencias.	X			X
	7.3	Toma de conciencia.	X			X
	7.4	Comunicación	X			
	7.5	Información documentada.	X			
	A.7	SEGURIDAD DE RECURSOS HUMANOS				
	A.7.2.2	Concientización, educación y formación en seguridad de la información	X			

Fortalezas:

- Para el establecimiento del SGSI el Ministerio dispone de los recursos necesarios para que el sistema de gestión funcione y pueda llevarse a cabo según lo planeado. Se precisan y proporcionan los recursos necesarios para la implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información.

- Se ha definido la competencia del personal para llevar a cabo las tareas del SGSI, centrándose en determinar la competencia necesaria del personal para llevar a cabo el trabajo que lo afecta. Se asegura que las personas sean competentes sobre la base de la educación, capacitación y experiencia necesarias. Se demostró que mediante la información documentada se cumple con los requisitos de la competencia del personal en materia de Seguridad de la Información.

Oportunidades de Mejora:

- **OM08.** Evaluar la eficacia de las acciones tomadas después de realizar las capacitaciones formativas, de entrenamiento y práctica, para verificar el mejoramiento de las competencias en el desempeño de la gestión de seguridad de la información. (Numeral 7.2.c).

- **OM09.** Incluir en las capacitaciones de seguridad de la información las lecciones aprendidas de los incidentes de seguridad, para enriquecer y fortalecer el desempeño del Sistema de Gestión de Seguridad de la Información – SGSI (Numeral 7.3.b).

2.6 Sesión de Auditoría SGSI-06

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Dominio de Control A.9 Control de Acceso y A.10 Criptografía.

Criterios de Auditoría:
Objetivos de Control: A.9.1 Requisitos del negocio para control de acceso; A.9.2 Gestión de acceso a usuarios; A.9.3 Responsabilidades de los usuarios; A.9.4 Control de acceso a sistemas y aplicativos; A.10.1 Política de uso de controles criptográficos; A.10.2 Gestión de claves.

CICLO DEL PROCESO	REQUISITO A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.9	CONTROL DE ACCESO.				
	A.9.1	Requisitos del negocio para control de acceso.	X			
	A.9.2	Gestión de acceso a usuarios.	X			
	A.9.3	Responsabilidades de los usuarios.	X			
	A.9.4	Control de acceso a sistemas y aplicativos.	X			
	A.10	CRIPTOGRAFÍA				
	A.10.1	Política de uso de controles criptográficos	X			X
	A.10.2	Gestión de claves	X			

Fortalezas:

- La conexión remota a la red de área local del MEN está establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual es autorizada por la OTSI, en la que se cuenta con el monitoreo y registro de las actividades necesarias. La autenticación de usuarios remotos es aprobada por el jefe inmediato del usuario previa solicitud diligenciada, en su respectivo formato, a la mesa de ayuda de tecnología. Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

- Desde el área o proceso se solicita la creación de los usuarios y los privilegios de acceso al sistema de información. Se cuenta con un proceso de inactivación o eliminación de usuarios por medio de un formato de paz y salvo, donde en personal debe pasar por el proceso de OTSI. Se controla el cumplimiento de las políticas de seguridad de la información en el uso y selección de las contraseñas de acceso, por lo que se hacen responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados. Todo equipo de cómputo que requiera acceso a la red interna del MEN tiene como mínimo las medidas de seguridad: solución de antimalware instalada y actualizada, parches de seguridad al día y mecanismos de autenticación habilitado para el ingreso a la red (ISE).

Oportunidades de Mejora:

- **OM10.** Se requiere desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información que tenga en cuenta el ciclo de vida completo: generación, uso y protección, distribución, renovación y destrucción. Objetivo de Control A.10.1.1.

2.7 Sesión de Auditoría SGSI-07

Objetivo:

Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013. Dominio de Control A.11 Seguridad Física y Ambiental.

Criterios de Auditoría:

Objetivos de Control A.11.1 Áreas seguras y A11.2 Equipos.

CICLO DEL PROCESO	REQUISITO A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.11	SEGURIDAD FÍSICA Y AMBIENTAL				
	A.11.1	Áreas Seguras	X			
	A.11.2	Equipos	X			

Fortalezas:

- Los Data Center del MEN están instalados en un centro de datos principal y otro está sujeto a cambios según el Acuerdo Marco de Precios (AMP); éstos cuentan con capacidades de respaldo de energía ininterrumpida, ajustados a la capacidad de cada uno, sistemas de control de acceso, seguridad perimetral, sistemas de detección y prevención de incendios, cableado estructurado, conexión mediante fibra oscura entre centros de datos, monitoreo, plataformas tecnológicas de respaldo y virtualización, redes y comunicaciones.

- La plataforma tecnológica (Hardware, software y comunicaciones) cuenta con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados. Se tienen instalados sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se protege la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

2.8 Sesión de Auditoría SGSI-08

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A.12. Seguridad en las Operaciones.
Criterios de Auditoría:
Objetivos de Control A.12.1 Procedimientos y responsabilidades operacionales; A.12.2 Protección contra malware; A.12.3 Backups de la información; A.12.4 Registro y supervisión; A.12.5 Control de software de producción; A.12.6 Gestión de vulnerabilidades técnicas y A.12.7 Consideraciones técnicas de auditoría de sistemas.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.12	SEGURIDAD EN LAS OPERACIONES.				
	A.12.1	Procedimientos y responsabilidades operacionales.	X			X
	A.12.2	Protección contra malware.	X			
	A.12.3	Backups de la información.	X			
	A.12.4	Registro y supervisión.	X			
	A.12.5	Control de software de poducción.	X			
	A.12.6	Gestión de vulnerabilidades técnicas.	X			
	A.12.7	Consideraciones técnicas de auditoría de sistemas.	X			

Fortalezas:

- El procedimiento de gestión de cambios especifica los canales autorizados para la recepción de solicitudes de cambios, como la mesa de servicios, el correo electrónico o un oficio dirigido al líder de tecnología de la información. Se establece y se aplica el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware. Los cambios realizados sobre los sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumple satisfactoriamente.

- La infraestructura de procesamiento de información del Ministerio, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. El MEN cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso; el servicio es administrado por la OTSI. Los equipos de terceros que son autorizados para conectarse a la red de datos del Ministerio deben tener antivirus y contar con las medidas de seguridad apropiadas.

Oportunidades de Mejora:

- **OM11.** Dentro de la creación de procedimientos operativos documentados para gestión de seguridad de TI, se puede incluir lo relacionado con servicios de terceros, manejo de errores y condiciones excepcionales que pueden definirse como incidentes de seguridad, transferencia de información e instrucciones especiales de manejo de medios para información confidencial. (Objetivo de Control A.12.1.1).

2.9 Sesión de Auditoría SGSI-09

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A13. Seguridad de Comunicaciones.

Criterios de Auditoría:
Objetivos de Control A.13.1 Gestión de la seguridad de las redes y A.13.2 Transferencia de información.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.13	SEGURIDAD DE COMUNICACIONES				
	A.13.1	Gestión de la seguridad de las redes.	X			
	A.13.2	Transferencia de información.	X			

Fortalezas:

- La Oficina de Tecnología y Sistemas de Información tiene implementados controles a la mensajería electrónica como: protección ante acceso no autorizado (mensajes encriptados), aseguramiento al correcto direccionamiento y transporte de los mensajes; confiabilidad y disponibilidad del servicio; consideraciones legales (firmas digitales); exigibilidad de autorización de uso de servicios públicos externos (mensajería instantánea, redes sociales y compartir archivos), y medidas adicionales de autenticación en accesos desde redes públicas.

- Existen acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección. Para realizar intercambio de información de propiedad del Ministerio con otras entidades, se sigue un proceso formal de requisición de la información, el cual debe contar con autorización previa del dueño de la información.

2.10 Sesión de Auditoría SGSI-10

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A.14. Desarrollo, Adquisición y Mantenimiento de Sistemas.

Criterios de Auditoría:
Objetivo de Control A.14.1 Requisitos de seguridad de los sistemas de información; A.14.2 Seguridad de los procesos de desarrollo y de soporte; A.14.3 Datos de prueba.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.14	DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS				
	A.14.1	Requisitos de seguridad de los sistemas de información	X			
	A.14.2	Seguridad de los procesos de desarrollo y de soporte	X			X
	A.14.3	Datos de prueba	X			X

Fortalezas:

- Los ambientes designados para los sistemas de información de Ministerio tienen políticas de seguridad que se derivan desde la definición y gestión de la infraestructura tecnológica. El MEN cuenta con ambientes de certificación y producción. Los ambientes de desarrollo y pruebas son responsabilidad de los fabricantes/ proveedores (incluyendo la fábrica de software).

Oportunidades de Mejora:

- **OM12.** Implementar la política de desarrollo seguro y los procedimientos pertinentes. Objetivo de Control A.14.2.1.

- **OM13.** Los entornos de pruebas no siempre cuentan con los mismos niveles de seguridad de la información que los entornos de operación, por lo que se requiere establecer controles de selección de datos para los sistemas de prueba y para entornos de desarrollo. Objetivo de Control A.14.3.1.

2.11 Sesión de Auditoría SGSI-11

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A.15. Relación con Proveedores.

Criterios de Auditoría:
Objetivos de Control A.15.1 Seguridad de la información en las relaciones con los proveedores; A.15.2 Gestión de la prestación de servicios de proveedores.

CICLO DEL PROCESO	REQUISITO /CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.15	RELACIÓN CON PROVEEDORES				
	A.15.1	Seguridad de la información en las relaciones con los proveedores	X			
	A.15.2	Gestión de la prestación de servicios de proveedores	X			X

Fortalezas:

- Se tiene establecida una administración delegada de los sistemas de información del Ministerio, bajo un servicio provisto por el Proveedor, que incluye operación del servicio, gestión de aplicaciones y gestión técnica de infraestructura TI, de acuerdo con los alcances que se definen dentro del anexo técnico. Así mismo, se tiene definido el servicio de optimizar la utilización de los recursos actuales y adquirir por el Ministerio la infraestructura TI del MEN, que incluye soluciones de seguridad, balanceadores, monitoreo y backups, soluciones LaaS, PaaS y SaaS. Se cuenta con un modelo de servicio flexible y servicios por demanda.

Oportunidades de Mejora:

- **OM14.** Se pueden establecer criterios de seguridad de la información para cada servicio, producto o tecnología de comunicación a subcontratar. La evaluación de riesgos enfocada a un servicio o producto en concreto, ayuda a adoptar los criterios a la hora de subcontratar este servicio y determinar qué características o nivel de seguridad requiere a la hora de elegir al contratista. Se definen las cláusulas para el subcontratista dirigidas a la aplicación de requisitos de seguridad a sus proveedores y a toda la cadena de suministro. Objetivo de Control A.15.2.2.

2.12 Sesión de Auditoría SGSI-12

Objetivo:

Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A.16 Gestión de Incidentes de Seguridad de la Información.

Criterios de Auditoría:

Dominio de Control A.16.1 Gestión de incidentes y mejoras en la seguridad de la información.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A. 16	GESTIÓN DEINCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				
	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información.				
	A.16.1.1	Responsabilidades y procedimientos	X			
	A.16.1.2	Reporte de eventos de seguridad de la Información	X			
	A.16.1.3	Reporte de debilidades en seguridad de la información	X			
	A.16.1.4	Evaluación y decisiones en eventos de seguridad	X			
	A.16.1.5	Respuesta a incidentes de seguridad de la información	X			
	A.16.1.6	Aprendizaje de los incidentes de seguridad	X			
	A.16.1.7	Recolección de la Evidencia	X			X

Fortalezas:

- Se realizan pruebas de penetración o pentesting para identificar debilidades de seguridad sobre un servidor, una aplicación, etc. Estas pruebas permiten comprobar los controles de seguridad las aplicaciones Web, detectando vulnerabilidades que un atacante podría explotar, y posteriormente introduciendo los correctivos de remediación y neutralización de la amenaza.

- Se realizan reuniones técnicas para revisar los incidentes de seguridad informática y definir planes de tratamiento de riesgos de acuerdo con las recomendaciones del proveedor.

Oportunidades de Mejora:

- **OM15.** Definir y aplicar procedimientos en el SGSI para la identificación, recolección, adquisición y preservación de la información asegurando la cadena de custodia en las evidencias digitales, apoyándose en la Guía 13 - Evidencia Digital del MSPI del MinTIC, la cual da los lineamientos para realizar un proceso de informática forense adecuado, siendo a su vez un complemento al proceso de gestión de incidentes de seguridad de la información establecido dentro del MEN. Objetivo de Control A.16.1.7.

2.13 Sesión de Auditoría SGSI-13

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A.17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.
Criterios de Auditoría:
Objetivos de Control A.17.1 Continuidad de la seguridad de la información; A17.2 Redundancias.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A. 17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
	A.17.1	Continuidad de la seguridad de la información	X			
	A.17.2	Redundancias.	X			X

Fortalezas:

- El Ministerio a través de su Política de Gestión de Continuidad de Negocio, establece los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis. El Ministerio cuenta con un centro de datos alterno, para garantizar la disponibilidad de los servicios críticos de la entidad, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.

Oportunidades de Mejora:

- **OM16.** Realizar monitoreo y seguimiento periódico del consumo de recursos de las VSAN, con el fin de identificar si por requerimientos del servicio las capacidades dejan de ser suficientes para soportar la carga en un solo centro de datos (Análisis de Impacto – BIA). Objetivo de Control A.17.2.1.

2.14 Sesión de Auditoría SGSI-14

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Dominio de Control A.18 Cumplimiento y Numeral 9. Evaluación de Desempeño.
Criterios de Auditoría:
Objetivos de Control: A.18.1 Cumplimiento de requisitos legales y contractuales; A.18.2 Revisiones de seguridad de la información.
Requisitos de Norma: 9.2 Auditoría Interna y 9.3 Revisión por la dirección.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
HACER	A.18	CUMPLIMIENTO				
	A.18.1	Cumplimiento de requisitos legales y contractuales	X			X
	A.18.2	Revisiones de seguridad de la información.	X			
VERIFICAR	9.	EVALUACIÓN DE DESEMPEÑO				
	9.2	Auditoría interna	X			
	9.3	Revisión por la dirección.	X			

Fortalezas:

- Actualmente el Ministerio tiene procedimientos que garantizan el uso del software de acuerdo con los términos previstos en la Ley de Propiedad Intelectual; para ello, se establecen algunos puntos a tener en cuenta para cumplir con este control, se dispone de una política de uso legal de productos de Software, asegurando la no violación de derechos de propiedad intelectual, se mantiene la política de licencias del Software, se controla el número máximo de usuarios por licencia y se revisa periódicamente que se estén utilizando solamente productos de Software con licencia.

- El Ministerio establece la política y lineamientos para la seguridad de la información, y para el tratamiento y confidencialidad de datos personales por parte del MEN. La Política es aplicable a toda la información contenida en las diferentes bases de datos que se obtienen a través de los sistemas de información con que cuenta el MEN, específicamente los datos de la población vinculada al sistema educativo de preescolar, básica, media, educación para el trabajo y el desarrollo humano y educación superior en virtud de la función que, como garante del servicio público educativo compete a este Ministerio. El Ministerio realizó el Registro Nacional de Base de Datos - RNBD a través de la Oficina de Planeación y la Oficina de Tecnología y Sistemas de Información – OTSI.

- Se llevan a cabo auditorías específicas por la Oficina de Control Interno en intervalos planificados para verificar la gestión de seguridad y privacidad de la información en los activos de TI, registrando su resultado en el Sistema Integrado de Gestión – SIG, en consonancia con la estrategia de Gobierno Digital establecida en el Decreto 1078 de 2015 y el avance del Modelo de Seguridad y Privacidad de la Información – MSPI.

- A través de los Comités de Revisión de la Dirección: Comité de Dirección, Comité Institucional de Gestión y Comité de Desempeño, se informa trimestralmente al Ministerio sobre el desempeño del SGSI y sus acciones de mejora. Se revisan los planes de acción institucional y estratégicos de MIPG, incluyendo los resultados del reporte realizado en FURAG y del EDI. (Acta Comité 26 marzo-2019 - PM-FT-01 v3).

Oportunidades de Mejora:

- **OM17.** Establecer la Política de Derechos de Propiedad Intelectual y la Política de Controles criptográficos, teniendo en cuenta las responsabilidades y aplicabilidad de los controles criptográficos dentro de la operación. Objetivo de Control A.17.2.1.

2.15 Sesión de Auditoría SGSI-15

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Numeral 9. Evaluación de Desempeño.

Criterios de Auditoría:
Requisito de Norma 9.1. Seguimiento, medición, análisis y evaluación.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
VERIFICAR	9	EVALUACIÓN DE DESEMPEÑO				
	9.1	Seguimiento, medición, análisis y evaluación	X			

Fortalezas:

- Para el proceso de Gestión de Servicios TIC, en el Sistema Integrado de Gestión – SIG se tiene la alineación de los objetivos estratégicos con el modelo referencial del Sistema de Gestión de Seguridad de la Información – SGSI, definidos cuatro (4) objetivos específicos:

  1. Aumentar el nivel de implementación del Plan de Seguridad y Privacidad de la Información, 2. Consolidar una cultura de seguridad de la información en los colaboradores y terceros de la entidad, 3. Identificar y gestionar los riesgos a los cuales se expone la información, fortaleciendo la confidencialidad, integridad y disponibilidad de la misma en la entidad, así como la continuidad de las operaciones del MEN y, 4. Consolidar la eficiencia del SGSI mediante la implementación de los controles de seguridad de la información protegiendo la entidad frente a las amenazas internas o externas.

  La meta de los indicadores 1. Avance en la implementación del Plan de Seguridad y Privacidad de la Información (meta 90%), 2. Ejecución del Plan de Comunicaciones del SGSI (meta 80%), 3. Procesos con riesgos de seguridad de la información gestionados (meta 80%) y 4. Implementación de controles de seguridad de la información (meta 80%), respectivamente. En el acta del Comité Institucional Virtual No.12 mayo 2020 se registra el avance del Plan de Seguridad y Tratamiento de Riesgos del SGSI.

- De acuerdo con la Resolución N. 01760 de 2018, se actualiza la regulación del SIG del MEN, estableciendo los roles, funciones e instancias decisorias de conformidad con las normas vigentes de gestión y desarrollo institucional, considerando al SIG la herramienta gerencial que promueve y facilita la mejora continua en la gestión, orientada a lograr el cumplimiento de los requisitos normativos relacionados con cada modelo referente y con los determinados en el Modelo Integrado de Planeación y Gestión - MIPG.

2.16 Sesión de Auditoría SGSI-16

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Numeral 9. Evaluación de Desempeño.

Criterios de Auditoría: Requisito de Norma 9.3 Revisión por la dirección.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
VERIFICAR	9	EVALUACIÓN DE DESEMPEÑO				
	9.3	Revisión por la dirección	X			

Fortalezas:

- Se tiene establecido en el Ministerio el Procedimiento de Revisión por la Dirección – PM-PR-04 v4, como un mecanismo de verificación y cumplimiento del Sistema Integrado de Gestión –SIG (Modelos Referenciales: Calidad, Ambiental, Seguridad de la Información y Seguridad, Salud en el Trabajo), en el cual se evalúa su eficacia, conveniencia e identificación de posibles cambios en el sistema, así como oportunidades de mejora. La revisión por la dirección se lleva a cabo como mínimo una vez al trimestre. Así mismo, se revisan y analizan cada uno de los componentes e insumos de información del Sistema Integrado de Gestión, de forma constante y en los diferentes espacios que el MEN tiene establecidos para el seguimiento y monitoreo del SIG.

2.17 Sesión de Auditoría SGSI-17

Objetivo:
Comprobar que el SGSI implementado cumple con los requisitos de norma NTC ISO/IEC 27001:2013 Numeral 10. Mejora.

Criterios de Auditoría:
Requisitos de Norma: 10.1 No conformidades y acciones correctivas y 10.2 Mejora continua.

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO			
			C	HZ	NC	OM
ACTUAR	10	MEJORA				
	10.1	No conformidades y acciones correctivas	X			
	10.2	Mejora continua	X			

Fortalezas:

- Se tiene establecido en el Ministerio el Procedimiento de Gestión de Planes de Mejoramiento – PM-PR-02 v4, y a través del Sistema del SIG registrar y realizar seguimiento de las acciones correctivas, preventivas y/o de mejora del plan de mejoramiento respectivo, bajo la responsabilidad de los líderes de los procesos de las dependencias encargadas de ejecutar las acciones de la mejora y el apoyo de la Subdirección de Desarrollo Organizacional – SDO en la generación de alertas.

- Actualmente, se tienen en el Sistema Integrado de Gestión - SIG, siete (7) submódulos del SGSI: 1. Activos; 2. Declaración de Aplicabilidad; 3. Gestión de Incidentes; 4. Plan de Continuidad; 5. Gestión de Vulnerabilidades; 6. Reportes y 7. Gestión de Riesgos, de los cuales se tiene como meta para este año la implementación de los submódulos de Gestión de Activos y Gestión de Riesgos.

3. CONCLUSIONES

Evaluado el Proceso de Gestión de TIC como alcance del Modelo Referencial del Sistema de Gestión de Seguridad de la Información – SGSI de Ministerio de Educación Nacional, conforme a la norma técnica NTC ISO/IEC 27001:2013, se concluye que:

- Existe una fuerte gestión tecnológica de la información, con énfasis en la seguridad informática, basada en medios y tecnología de punta, que le ha permitido al Ministerio responder (en mayor medida y con seguridad razonable) a los retos y amenazas actuales del entorno.

- El Sistema de Gestión de Seguridad de la Información – SGSI está en su fase de implementación, en consonancia con el Sistema Integrado de Gestión – SIG y el Modelo Institucional de Planeación y Gestión – MIPG, convirtiéndose en una herramienta de apoyo en la organización de procesos, controles y salvaguardas con los que se mantiene la información bajo medidas de seguridad para garantizar su integridad, confidencialidad, autenticidad y disponibilidad.

- Se ha logrado el objetivo y alcance de la auditoría interna combinada y se puede concluir, con base en la muestra auditada, que el proceso carece de *"no conformidades"* con respecto a los requisitos de la norma técnica NTC ISO/IEC 27001:2013 y demás criterios aplicados, no obstante haber detectado durante la auditoría diecisiete (17) oportunidades de mejora.

- Se evidencia el avance en la implementación de controles definidos para el Sistema de Gestión de Seguridad de la Información - SGSI del Ministerio de Educación Nacional, reflejado en el indicador del MSPI Gobierno Digital del 80% para el 2019 y del 85% para 2020; sin embargo, se observan las oportunidades de mejora ya citadas, en cuanto a: documentación, procedimiento, mapa de riesgos y controles del sistema, las cuales requieren ser gestionadas.

- Procede fortalecer los mecanismos metodológicos internos de valoración y tratamiento de riesgos de seguridad de la información, con el fin de ser concordantes e integrados al sistema general de riesgos, pues son la base fundamental de los sistemas de gestión que el Ministerio adopte.

- Es importante evaluar la declaración de aplicabilidad de los controles de seguridad de la información del Ministerio como parte del Sistema de Gestión de Seguridad de la Información, para definir los mecanismos de control a implementar.

4. RECOMENDACIONES

- Mantener el compromiso de la Subdirección de Desarrollo Organizacional – SDO, la Oficina de Control Interno – OCI y la Oficina de Tecnología y Sistemas de Información – OTSI, con el mejoramiento continuo de la gestión de seguridad de la información y con el cumplimiento de las regulaciones y normas relacionadas con el fortalecimiento de la gestión TIC del sector educativo.

- Analizar, priorizar e implementar las acciones necesarias que realicen las oportunidades de mejora identificadas y las de los informes de seguimiento, derivadas de los informes de los proveedores sobre planes de seguridad informática, gestión de vulnerabilidades operativas, disponibilidad de dispositivos de seguridad, gestión de identidad y acceso, y cumplimiento del modelo operativo y del plan de actualización tecnológica, con el fin de prevenir daños por potenciales amenazas, de forma que se eviten no conformidades en el futuro.

AUDITOR LÍDER: Clara Patricia Muñoz Jiménez

JEFE OFICINA DE CONTROL INTERNO: María Helena Ordóñez Burbano