Educación	**INFORME DE AUDITORÍAS**	**Código:** EI–FT-02 **Versión:** 01 Rige a partir de su publicación en el SIG

Proceso: Gestión de Servicios Tic

Política __, Plan__, Programa __, Proyecto __, Procedimiento __ y/o Actividad __

AUDITORÍAS DE GESTIÓN-SISTEMA DE CONTROL INTERNO (MIPG-AUDITORÍA BASADAS EN RIESGOS)-2025

Número de Auditoría: 2025-G-03

Fecha Reunión de Apertura: 03/07/2025

Fecha Reunión de Cierre: 30/09/2025

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S)
CAMILO ERNESTO CARVAJALINO MARTA

EQUIPO AUDITOR

AUDITOR LIDER:	WILLIAM MONROY RINCON
AUDITORES :	SANDRA MILENA PERDOMO HERRERA
	BLANCA LILIA PORRAS MELO

OBJETIVO DE AUDITORÍA:

Evaluar el cumplimiento de los requisitos establecidos por la norma ISO/IEC 27001:2013 y los de la transición a la 27001:2022 en materia de seguridad de la información: Para verificar la efectividad de los procedimientos, formatos y bitácoras del SGSI. Monitorear el avance de los planes de manejo de riesgos, los indicadores tecnológicos del Plan de Acción Institucional (PAI), el presupuesto, la contratación y la gestión de PQRSD asociados al Proceso Gestión de Servicios TIC del Ministerio de Educación Nacional.

ALCANCE DE AUDITORÍA

En la auditoría, se evaluaron los siguientes aspectos:

1. Cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001:2013 y los de la transición 27001:2022 de Seguridad de la Información.
2. Procedimientos de Gestión de Seguridad de la Información, ST-PR-08 – Versión 4, Gestión de incidentes de seguridad de la información - ST-PR-18 – Versión 2.
3. Revisión de los formatos de bitácoras de eventos ST-FT-21 – Versión 1, Roles y Responsabilidades en Seguridad de la Información, ST-FT-15 – Versión 1.
4. Manual de gestión de incidentes de seguridad de la información, ST-MA-04 – Versión 1.
5. Seguimiento al avance de los planes de manejo de riesgos de proceso y corrupción asociados al Proceso de Gestión de Servicios TIC.

6. Plan de Acción Institucional PAI 2024:
   Seguimiento a los indicadores de gestión de conectividad escolar, monitoreo del rendimiento de aplicaciones y transformación digital.
7. Inspección del presupuesto definido para el Proceso Gestión de Servicios TIC
8. Análisis de contratación con énfasis en cumplimiento de perfiles del personal técnico exigido y la ejecución contractual del Proceso Gestión de Servicios TIC.
9. Revisión de acciones tomadas frente a la gestión de PQRSD conforme a la Resolución 15908 de 2017 de la Oficina de Tecnología y Sistemas de Información.

Periodo para analizar corresponde a partir del 15 de agosto de 2024 hasta el 30 de junio de 2025

CRITERIOS DE AUDITORÍA:

1. Cumplimiento de los requisitos establecidos en la norma Seguridad de la Información/ISO IEC 27001:2013 y transición 2022.
2. Procedimiento de Gestión de incidentes de seguridad de la información - ST-PR-18.
3. Procedimiento ST-PR-15 de monitoreo y gestión de eventos, revisión del uso del formato ST-FT-21.
4. Seguimiento al avance de los planes de manejo de riesgos de servicios TIC.
5. Revisión de acciones tomadas frente a la gestión de PQRSD conforme a la Resolución 15908 de 2017.
6. Plan de Acción Institucional PAI 2024
7. Seguimiento a compromisos de conectividad escolar, monitoreo del rendimiento de aplicaciones y transformación digital.
8. Análisis de contratación TIC con énfasis en cumplimiento de perfiles del personal técnico exigido y supervisión contractual.

RESUMEN GENERAL

I. FORTALEZAS

El Ministerio de Educación Nacional cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) estructurado, lo que se refleja en la existencia de políticas, procedimientos y formatos formalmente documentados y publicados en el Sistema Integrado de Gestión (SIG).

Se destaca la protección de la infraestructura física mediante sistemas de climatización de precisión que controlan temperatura y humedad. Además, se realizan mantenimientos preventivos semestrales en racks, cableado estructurado y equipos auxiliares para asegurar condiciones óptimas de operación.

La gestión de cambios en servidores se maneja de manera formal con solicitudes de cambio (RFC) revisadas por un comité especializado, asegurando la trazabilidad, el análisis de riesgos y la autorización de modificaciones en la infraestructura.

El esquema de respaldos es sólido y contempla diferentes frecuencias de ejecución y periodos de retención.

La gestión de continuidad del negocio se refuerza con un plan de recuperación ante desastres en proceso de validación, incluyendo acciones para garantizar la disponibilidad de servicios críticos. También se gestionan y documentan incidentes de seguridad, asegurando la preparación y respuesta ante eventos adversos.

Indicadores institucionales con buenos resultados:
- Transformación digital alcanzó la meta de 90% en 2024 y un 50% de avance para el 2025 con proyectos estratégicos en analítica, automatización y robotización.
- Monitoreo de aplicaciones críticas alcanzó el 100% en 2024 con 8 aplicaciones priorizadas y en 2025 avanza con un 50%, garantizando estabilidad y disponibilidad en las aplicaciones monitoreadas.
- Conectividad escolar logró un 74% en 2024 con 71 secretarías viabilizadas y en 2025 avanza con un 52% al primer semestre, fortaleciendo el acompañamiento técnico y la cobertura.

Los controles cubren áreas como seguridad física, controles técnicos, gestión de incidentes, continuidad del negocio, seguridad en proveedores, y ahora también inteligencia de amenazas, resiliencia, nube y tecnologías emergentes.

II. COMPONENTES DE RIESGOS Y EVALUACIÓN DE CONTROLES

La Oficina de Control Interno, en el marco de la auditoría realizada, evaluó la identificación y el diseño de los controles asociados a los riesgos definidos en el proceso de Servicios TIC, validando los mismos de acuerdo con el alcance establecido para la auditoría:

Riesgo de Gestión:

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
		PREVENTIVO: El operador valida los servicios tecnológicos, generando un informe de disponibilidad con una		Al analizar el seguimiento de los controles se evidencia para el Tercer trimestre del 2024: se observó una adecuada identificación del control, en el monitoreo se evidencia el Informe SSP Reporte De Disponibilidad SERVICIOS TIC Contrato número CO1.PCCNTR.4356332 de 2022

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
Posibilidad de pérdida reputacional y económica por omisiones y/o deficiencias en la prestación del servicio que ofrece el ministerio a sus grupos de valor, debido a la	**PROBABILIDAD** MUY BAJA (20%) **IMPACTO** CATASTRÓFICO (100%) **EVALUACIÓN** Zona de Riesgo EXTREMA	periodicidad mensual con rezago de un mes, a través del ST-FT-26 Formato Plan de Disponibilidad incluido en el Procedimiento Gestión de Disponibilidad	**PROBABILIDAD** MUY BAJA (20%) **IMPACTO** CATASTRÓFICO (100%) **EVALUACIÓN** Zona de Riesgo EXTREMA	INFOTIC del mes de junio 2024 versión 2 del 10 de julio de 2024, de julio de 2024 versión 1 del 01 de agosto de 2024 y del mes de agosto 2024 versión 1 del 01 de septiembre de 2024. Cuarto trimestre del 2024: Durante el cuarto trimestre de 2024, se evidenció que el operador realizó el monitoreo de los servicios tecnológicos, por medio de los informes de disponibilidad. Primer Semestre del 2025 se observó una adecuada identificación del control, en el monitoreo se evidencia tres informes mensuales de disponibilidad servicios TI SSP de Enero, Febrero y marzo de 2025 CO1.PCCNTR.7095293 LOTE 2 de SELCOMP, con un detallado seguimiento al networking, bases de datos y servidores, además incluyen recomendaciones preventivas. Segundo trimestre del 2025: Se evidencia los informes correspondientes a los meses de abril, mayo y junio de 2025 como parte del contrato CO1.PCCNTR.7095293 LOTE 2 de SELCOMP. Para abril de 2025, el promedio de disponibilidad alcanzado fue del 99,97%, presentándose incidentes en los servidores HPC (IN948171 e IN948247) que, aunque generaron reinicios de máquinas virtuales, fueron gestionados de manera oportuna. En mayo de 2025, la disponibilidad promedio fue de 99,99%, destacándose un incidente relacionado con la base de datos MySQL (IN944957) y un fallo en el disco que afectaron temporalmente la sincronización del clúster. Finalmente, en junio de 2025, la disponibilidad

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
indisponibilidad de los servicios de TI				promedio fue de 99,98%, registrándose incidentes en servidores de Web Hosting y un reinicio inesperado de un servidor ESXi
		PREVENTIVO: Las coordinaciones de Aplicaciones e Infraestructura verifican trimestralmente la actualización del inventario de aplicaciones, dejando evidencia en la matriz establecida para tal fin.		Tercer trimestre del 2024: se observó una adecuada identificación del control, en el monitoreo se evidencia el documento InventarioAPPsV17530092024 que corresponde al inventario de aplicaciones. Cuarto trimestre del 2024: Durante el cuarto trimestre del año, se evidenció los profesionales de la OTSI responsables de las coordinaciones del grupo de aplicaciones e infraestructura, verificaron la actualización del inventario de aplicaciones. Primer Semestre del 2025 se observó una adecuada identificación del control, en el monitoreo se evidencia Matriz de Compatibilidad Aplicaciones, con la que verificaron de manera trimestral los Procedimiento Gestión Catálogo de Servicios y Niveles de Servicio. Segundo trimestre del 2025: Se evidencia Matriz Compatibilidad Junio 2025, el cual contienen información detallada sobre las aplicaciones, versiones de bases de datos, sistemas operativos y compatibilidad con estándares tecnológicos actuales. Se apreció que varias aplicaciones presentan versiones de bases de datos y sistemas operativos desactualizados, lo que ha sido anotado en las observaciones por el operador. Entre los casos destacados se encuentran aplicaciones que requieren

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
				migración a versiones superiores de PostgreSQL y actualizaciones de Red Hat Enterprise Linux, lo cual es fundamental para garantizar la compatibilidad y seguridad de los entornos tecnológicos. Asimismo, la matriz refleja la viabilidad técnica de las actualizaciones y la necesidad de considerar la compatibilidad con IPv6, identificando aquellas aplicaciones que actualmente no cumplen con este estándar.
		PREVENTIVO: El Comité de Cambios periódicamente revisa y aprueba la postulación de RFC con el propósito de realizar cambios en la infraestructura sin que afecten la disponibilidad de servicios, como evidencia se genera un acta de aprobación.		Tercer trimestre del 2024: se observó una adecuada identificación del control, en el monitoreo se evidencia el Informe de Efectividad de las órdenes de cambio de julio a septiembre de 2024. Cuarto trimestre del 2024: Durante el cuarto trimestre del año, se evidenció el profesional de seguridad informática analizó los RFC fallidos, para detectar omisiones o deficiencias, el cual fue registrado en el informe trimestral correspondiente. Primer Semestre del 2025: se observó una adecuada identificación del control, en el monitoreo se evidencia Actas de reunión del Comité de Cambios periódicamente de enero, febrero y marzo de 2025, donde periódicamente revisó y aprobó la postulación de RFC con el propósito de realizar cambios en la infraestructura sin que afecten la disponibilidad de servicios. Segundo trimestre del 2025: Se evidencia Actas de reunión del Comité de Cambios periódicamente de abril, mayo y junio de 2025, donde

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
				periódicamente evaluó y aprobó un número considerable de RFC en ambientes de producción, certificación y pruebas, abarcando actividades como actualizaciones de sistemas operativos, mantenimiento preventivo de infraestructura, instalación de nuevos servidores y mitigación de vulnerabilidades identificadas. Se resalta que, durante las sesiones, el Comité aplicó medidas de control adicionales, como la suspensión temporal de nuevas solicitudes a líderes con pendientes postimplementación superiores a tres RFC, para asegurar el cierre adecuado de las actividades previas y mitigar posibles impactos acumulados en la infraestructura.

Fuente: Plataforma SIG-Módulo Riesgos

El riesgo identificado se relaciona con la posibilidad de pérdida reputacional y económica ocasionada por deficiencias en la prestación de los servicios que ofrece el ministerio a sus grupos de valor debido a la indisponibilidad de los servicios de tecnologías de la información, siendo valorado como de probabilidad muy baja equivalente al 20 % pero con un impacto catastrófico del 100 % lo que lo ubica en una zona de riesgo extrema de acuerdo con la metodología establecida para la gestión de riesgos institucional.

El seguimiento realizado durante el tercer y cuarto trimestre de 2024 y el primer semestre de 2025 evidenció altos niveles de disponibilidad aproximados al 99,9 % y la existencia de controles efectivos como reportes periódicos, revisión de inventarios y gestión de cambios que han permitido atender oportunamente los incidentes presentados sin afectar la continuidad de los servicios.

Los informes de agosto y septiembre de 2024 confirmaron la estabilidad de los entornos tecnológicos con niveles superiores al 99,9 % y sin interrupciones significativas, mientras que en octubre se identificaron eventos asociados a la migración de PostgreSQL a la nube y a fallas en servidores de hiperconvergencia redujeron la disponibilidad a 99,47 %, los incidentes fueron atendidos sin impacto grave en la operación. Para noviembre se alcanzaron indicadores de hasta el 100 % de disponibilidad lo que demostró la capacidad de recuperación y la solidez de los mecanismos de control.

En el segundo trimestre de 2025 los informes de disponibilidad elaborados por el operador reportaron niveles superiores al 99,9 %, observándose en abril incidentes en servidores de alto rendimiento que generaron reinicios de máquinas virtuales, en mayo un evento en la base de datos MySQL y fallas en un disco que afectaron la sincronización de un clúster y en junio reinicios en servidores de web hosting y en un equipo de virtualización, situaciones que fueron atendidas de manera oportuna lo que permitió sostener la continuidad operativa sin afectaciones significativas.

De manera complementaria la revisión trimestral del inventario de aplicaciones realizada por las coordinaciones de Aplicaciones e Infraestructura mostró la necesidad de actualizar versiones de bases de datos y sistemas operativos, así como la incorporación progresiva de compatibilidad con el estándar IPv6, aspectos que resultan críticos para asegurar la disponibilidad de los entornos tecnológicos y prevenir riesgos asociados a obsolescencia o vulnerabilidades. A esto se suma la intervención del Comité de Cambios que evaluó y aprobó solicitudes relacionadas con modificaciones en infraestructura, actualizaciones y mantenimientos aplicando medidas de control como la restricción temporal de nuevas solicitudes a líderes con cambios pendientes de cierre, acción que contribuyó a fortalecer la estabilidad de los servicios y a reducir la posibilidad de acumulación de impactos en la operación.

Debido a que el Plan de Manejo No 2018 logró un cumplimiento del 100 % en las actividades programadas, razón por la cual se dio por cerrado. Como medida de continuidad y con el fin de mantener la efectividad de los controles implementados, se creó el Plan de Mejoramiento No 2412, orientado a reforzar la cultura de responsabilidad en la gestión de cambios. Este nuevo plan contempla la realización de sesiones semestrales de sensibilización dirigidas a los equipos responsables de los RFC, con el propósito de fortalecer la gobernanza, reducir la probabilidad de omisiones y garantizar la continuidad de los servicios, por lo cual, el plan registra un avance del 0 %, encontrándose en su fase inicial de ejecución.

Aunque la probabilidad de materialización del riesgo se mantiene baja el impacto potencial es crítico y conserva la clasificación en nivel extremo. Los controles implementados han mostrado efectividad en la mitigación de incidentes y en la garantía de continuidad de los servicios, sin embargo, el riesgo residual permanece alto debido a la dependencia tecnológica y a la necesidad de mantener procesos permanentes de actualización y compatibilidad con los estándares vigentes para reducir de manera sostenida la exposición

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
Posibilidad de pérdida económica y reputacional por	**PROBABILIDAD** MEDIA (60%) **IMPACTO**	**PREVENTIVO:** El líder de seguridad analiza el informe de resultado de	**PROBABILIDAD** BAJA (40%) **IMPACTO**	Al analizar el seguimiento de los controles se evidencia: Tercer trimestre del 2024 se observó una adecuada identificación del control, en el monitoreo se evidencia el Informe de resultado de

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
la indisponibilidad, alteración y/o afectación de la confidencialidad de la información contenida en los servicios de TI debido a ataques informáticos	MODERADO (60%) **EVALUACIÓN** Zona de Riesgo MODERADA	vulnerabilidades, con el propósito de gestionar las respectivas correcciones y alertas al respecto	MODERADO (60%) **EVALUACIÓN** Zona de Riesgo MODERADA	vulnerabilidades de julio a septiembre de 2024. Cuarto trimestre del 2024 Durante el cuarto trimestre del año 2024, se evidenció que la OTSI validó el resultado de vulnerabilidades y el cual se documentó el informe de vulnerabilidades. Primer Semestre del 2025 se observó una adecuada identificación del control, en el monitoreo se evidencia informes trimestrales Técnicos de Análisis de Vulnerabilidades APP255, APP322, APP348, APP 121 de CO1.PCCNTR.7095293 SELCOMP, los cuales registran análisis detallados de vulnerabilidades y realizan sugerencias para mejorar la postura de seguridad de la entidad ante amenazas. Segundo trimestre del 2025: se observó una adecuada identificación del control, en el monitoreo se evidencia Informe Técnico de Análisis y Remediación de Vulnerabilidades correspondiente al corte del 11 de julio de 2025, en el que se detalló la identificación de 4.852 vulnerabilidades en 396 activos críticos, de las cuales se remediaron 243 a la fecha de corte. Asimismo, se consignaron las actividades de análisis y priorización, enmarcadas en acciones correctivas inmediatas y planes de trabajo escalonados. Sin embargo, en el documento se identifican retos en la

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
				cobertura de remediación y en la implementación de métricas de gestión (MTTR, SLA).

Fuente: Plataforma SIG-Módulo Riesgos

Además, se detectó un riesgo asociado a la posibilidad de pérdida económica y reputacional por indisponibilidad, alteración o afectación de la confidencialidad de la información en los servicios de TI debido a ataques informáticos se mantiene en una zona moderada de exposición. La valoración inherente determinó una probabilidad media del 60 % y un impacto moderado del 60 %, estableciendo la necesidad de controles preventivos liderados por la gestión de vulnerabilidades.

Durante el tercer trimestre de 2024, el análisis de seguridad reveló un total de 9.428 vulnerabilidades en servidores de certificación y producción, con un alto porcentaje en categorías críticas y altas. En los equipos de seguridad se identificaron 98 vulnerabilidades adicionales, predominando las de nivel medio, lo que reflejó un entorno con riesgos persistentes en la infraestructura tecnológica.

En el cuarto trimestre del 2024, la tendencia de exposición se incrementó. Se detectaron 8.214 vulnerabilidades en octubre, 159 en noviembre y 13.104 en diciembre, destacando un crecimiento en hallazgos críticos y altos. Estos resultados mostraron un aumento significativo en la superficie de ataque y evidenciaron la necesidad de reforzar los procesos de remediación para evitar que los riesgos evolucionen hacia escenarios de materialización.

El seguimiento realizado para el primer semestre del 2025 confirma que los controles han sido implementados con regularidad, incluyendo el análisis de informes técnicos y la generación de planes de trabajo escalonados. No obstante, en el informe del 11 de julio de 2025 se registraron 4.852 vulnerabilidades en 396 activos críticos, de las cuales solo 243 habían sido remediadas, equivalente a un avance del 5 %. Aunque, se reconocen esfuerzos en análisis y priorización, persisten brechas en cobertura de remediación, ausencia de métricas importantes como MTTR y SLA, y falta de trazabilidad formal de las acciones, lo que limita la eficacia de los controles aplicados.

Si bien el riesgo no se materializó en los periodos evaluados, el crecimiento sostenido de vulnerabilidades críticas y el bajo nivel de remediación mantienen un nivel residual moderado que requieren atención prioritaria.

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
Posibilidad de pérdida económica y reputacional por la indisponibilidad, alteración y/o afectación de la confidencialidad de la información contenida en los servicios de TI debido a fallas en la infraestructura tecnológica.	**PROBABILIDAD** MEDIA (60%) **IMPACTO** CATASTRÓFICO (100%) **EVALUACIÓN** Zona de Riesgo EXTREMA	**PREVENTIVO:** El operador monitorea los servicios tecnológicos, generando un informe mensual de disponibilidad (con rezago de un mes) a través del ST-FT-26 Formato Plan de Disponibilidad incluido en el Procedimiento Gestión de Disponibilidad.	**PROBABILIDAD** BAJA (40%) **IMPACTO** CATASTRÓFICO (100%) **EVALUACIÓN** Zona de Riesgo EXTREMA	Al analizar el seguimiento de los controles se evidencia: Tercer trimestre del 2024 se observó una adecuada identificación del control, en el monitoreo se evidencia el Informe SSP Reporte de Disponibilidad SERVICIOS TIC Contrato número CO1.PCCNTR.4356332 de 2022 INFOTIC del mes de junio 2024 versión 2 del 10 de julio de 2024, del mes de julio de 2024 versión 1 del 01 de agosto de 2024 y del mes de agosto de 2024 versión 1 del 01 de septiembre de 2024 y los oficios del SGDEA enviados al gerente del proyecto con la aprobación de los informes. Cuarto trimestre del 2024 Durante el cuarto trimestre de 2024, se evidenció que el operador realizó el monitoreo de los servicios tecnológicos, por medio de los informes de disponibilidad. Primer Semestre del 2025 se observó una adecuada identificación del control, en el monitoreo se evidencia Informes de Disponibilidad de servicios TI SSP de Enero, Febrero y Marzo 2025 CO1.PCCNTR.7095293 SELCOMP, los cuales garantizan la continuidad operativa, y responden de manera oportuna ante incidentes que comprometan la estabilidad de los sistemas de la organización. Segundo trimestre del 2025:

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
				se observó una adecuada identificación del control, en el monitoreo se evidencia los informes de abril, mayo y junio 2025 con altos niveles de disponibilidad (99,98%) y uso de recursos dentro de umbrales normales, lo que demuestra la implementación del seguimiento, en su mayoría, garantizan la continuidad operativa y permiten responder de manera oportuna ante incidentes que comprometan la estabilidad de los sistemas institucionales. No obstante, se presentaron problemas críticos en servidores hiperconvergentes y de web hosting, relacionados con fallas físicas y sobrecarga de CPU, lo que confirma la persistencia de debilidades en componentes con vida útil superada, y constata la necesidad de fortalecer las más acciones preventivas y de renovación tecnológica.

Fuente: Plataforma SIG-Módulo Riesgos

El riesgo identificado por la OTSI corresponde a la posibilidad de pérdida económica y reputacional debido a la indisponibilidad, alteración o afectación de la confidencialidad de la información contenida en los servicios tecnológicos como consecuencia de fallas en la infraestructura de TI. Este riesgo, valorado inicialmente como de probabilidad media y con impacto catastrófico, ubica a la entidad en una zona de riesgo extremo, lo que exige la implementación de controles sólidos orientados a garantizar la continuidad de la operación y la protección de los activos de información críticos.

El control establecido por el MEN consiste en el monitoreo permanente de los servicios tecnológicos mediante informes de disponibilidad elaborados mensualmente, conforme al procedimiento de Gestión de Disponibilidad. Los reportes revisados evidencian niveles de servicio superiores al 99,9% en la mayoría de los componentes, lo que demuestra una gestión efectiva de la continuidad y del desempeño. No obstante, se identificaron incidentes asociados a fallas físicas y sobrecarga en servidores hiperconvergentes y de web hosting, lo que refleja la persistencia de vulnerabilidades en equipos cuya vida útil está superada. Esta situación confirma que, aunque el control mitiga en gran medida la probabilidad, el impacto potencial se mantiene alto y la clasificación del riesgo residual continúa en un nivel extremo.

Igualmente, se encuentra directamente relacionado con la operación y la continuidad de los servicios tecnológicos, ya que la debilidad en la infraestructura compromete la eficacia del sistema de control y aumenta la probabilidad de interrupciones graves. En consecuencia, es necesario reforzar las medidas preventivas a través de la renovación planificada de equipos críticos, la implementación de planes de contingencia más robustos y la integración de controles proactivos que permitan anticipar incidentes antes de que se conviertan en interrupciones significativas.

Debido a que el Plan de Manejo No 2017 logró un cumplimiento del 100 % en las actividades programadas, se dio por cerrado. Como medida de continuidad y con el fin de mantener la efectividad de los controles implementados, se creó el Plan de Mejoramiento No 2411, orientado a reforzar los controles de monitoreo y disponibilidad, por lo cual registra un avance del 0 % y se encuentra en estado en curso, lo que refleja que, aunque se han establecido las medidas preventivas, aún es indispensable avanzar en la renovación de componentes tecnológicos con vida útil superada para mitigar la causa raíz del riesgo.

Para terminar, se evidenció madurez en el cumplimiento de acuerdos de nivel de servicio, sin embargo, persiste un riesgo tecnológico que, de no ser tratado con acciones de modernización y fortalecimiento de la infraestructura, puede materializarse en eventos de impacto mayor que afecten la continuidad de los servicios críticos y la confianza de los usuarios en la organización.

Riesgo de Corrupción:

Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros por modificar, filtrar o extraer información reservada contenida en los diferentes sistemas de la Entidad.

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
		PREVENTIVO: El líder de seguridad suministra el informe de resultado de vulnerabilidades de manera trimestral y deja consignada la ejecución del análisis de vulnerabilidades y sus respectivas correcciones		Al analizar el seguimiento de los controles se evidencia para el Primer trimestre del 2025 se observó una adecuada identificación del control, en el monitoreo se evidencia los informes de vulnerabilidades APP 121, APP255, APP322 y APP348, presentados por el líder de seguridad en el tiempo establecido, los cuales detallan las amenazas encontradas, su nivel de riesgo y las soluciones

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros por modificar, filtrar o extraer información reservada contenida en los diferentes sistemas de la Entidad.	**PROBABILIDAD** RARA VEZ (1) **IMPACTO** CATASTRÓFICO (20) **EVALUACIÓN** **Zona de Riesgo EXTREMA**		**PROBABILIDAD** MUY BAJA (20%) **IMPACTO** CATASTRÓFICO (100%) **EVALUACIÓN** Zona de Riesgo EXTREMA	propuestas para su corrección. Segundo trimestre del 2025: se observó una adecuada identificación del control, por cuanto se evidencia informe técnico trimestral de análisis y remediación de vulnerabilidades, el cual documenta la identificación de 4.852 vulnerabilidades en 396 activos críticos del MEN, detallando brechas técnicas y de gestión, tales como baja cobertura de remediación en sistemas Windows y aplicaciones, problemas en la gestión de certificados y protocolos criptográficos, y falta de trazabilidad en los registros. Este informe evidencia la ejecución del análisis de vulnerabilidades y las acciones correctivas emprendidas, alineado con los estándares establecidos para mitigar riesgos que comprometan la seguridad de la información institucional.
		PREVENTIVO: El líder de seguridad elabora un informe mensual de control frente a inteligencia de amenazas con el propósito de dar alertas tempranas frente a ataques cibernéticos		Primer trimestre del 2025 se observó una adecuada identificación del control, en el monitoreo no hay evidencia de ejecución, debido a que el informe que anexan tan solo tienen los objetivos, no se puede apreciar la efectivamente del análisis de seguridad que contempla la tabla de contenido del documento como: inteligencia de amenazas recopiladas, infraestructura de ciberseguridad, eventos y hallazgos relevantes y correlación en SIEMSOC, no obstante, se recomienda dar cumplimiento a las fechas estipuladas en Circular 005 del 05 de febrero de 2025, donde las dependencias deben actualizar en el SIG el

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
				Reporte Monitoreo de riesgos hasta el 11042025. Segundo trimestre del 2025: se observó una adecuada identificación del control, por cuanto se evidencia informe mensual de inteligencia de amenazas, el cual presenta un análisis detallado del panorama de amenazas detectadas entre abril y junio de 2025, incluyendo vulnerabilidades críticas (como CVE20256543 y CVE202533053), intentos de ataque ransomware, campañas de phishing dirigidas a entidades públicas y el uso de técnicas avanzadas de evasión. Además, se documenta la efectividad de los controles existentes, como la correlación de eventos por parte del SOC, mecanismos de contención automatizados y acciones correctivas frente a incidentes detectados.
		PREVENTIVO: El líder de seguridad implementa de forma anual controles a nivel de Microsoft defender y deja consignado el resultado en un informe		Primer trimestre del 2025 se observó una adecuada identificación del control, en el monitoreo se evidencia el Plan de mejoramiento Despliegue de Microsoft Defender, el cual describe detalladamente fases implementadas, objetivos técnicos, cronograma, responsables y medidas de mitigación. El informe demuestra la implementación progresiva en estaciones de trabajo y servidores, la integración con SIEM, y la ejecución de simulaciones de ataques, fortaleciendo la capacidad de alerta temprana frente a amenazas cibernéticas. Segundo trimestre del 2025:

RIESGO	ANÁLISIS DEL RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ANÁLISIS DEL RIESGO RESIDUAL	OBSERVACIONES OCI
				se observó una adecuada identificación del control, por cuanto se evidencia la continuidad en el proceso de implementación anual de controles a nivel de Microsoft Defender, a través del informe del plan de despliegue presentado por la Oficina de Tecnología y Sistemas de Información. El documento describe de manera estructurada las fases del proyecto, contemplando preparación, piloto, despliegue masivo, integración con SIEM, validación y cierre, así como los objetivos específicos orientados a fortalecer la protección contra amenazas avanzadas.

Fuente: Plataforma SIG-Módulo Riesgos

El riesgo identificado por la OTSI, asociado a la posibilidad de recibir o solicitar beneficios indebidos con el fin de manipular, filtrar o extraer información reservada. Este riesgo representa un escenario de amenaza extrema para la entidad, dado que compromete la imagen institucional, puede generar pérdidas económicas y deteriora la confianza de los grupos de valor del MEN. Aunque la probabilidad se clasificó como poco frecuente, la severidad de sus consecuencias es catalogada como catastrófica, lo que sitúa el riesgo en una zona de prioridad máxima dentro del mapa de riesgos institucionales.

El monitoreo realizado en el segundo trimestre de 2025 evidenció que persisten debilidades estructurales en la gestión de vulnerabilidades. La identificación de 4.852 distribuidos en 396 activos críticos, con baja cobertura de remediación en sistemas Windows y aplicaciones, fallas en la administración de certificados y protocolos criptográficos y ausencia de trazabilidad en los cierres, configura un panorama de alto riesgo operativo. Estas condiciones abren la posibilidad de accesos indebidos, alteración de información sensible o fuga de datos, escenarios que elevan la exposición al riesgo de corrupción digital al facilitar la manipulación y/o uso inapropiado de activos institucionales.

No obstante, se reconoce que la entidad ha fortalecido mecanismos de control complementarios. La generación mensual de informes de inteligencia de amenazas ha permitido identificar intentos de ransomware, campañas de suplantación focalizadas y vulnerabilidades críticas de alcance internacional. Dichos reportes han sido aprovechados por el centro de operaciones de seguridad para ejecutar correlaciones de eventos, activar respuestas

automatizadas y aplicar medidas correctivas oportunas, reduciendo la ventana de exposición frente a incidentes.

A este esfuerzo se suma la implementación anual de controles mediante Microsoft Defender, con un plan estructurado que contempla fases de despliegue, integración con sistemas de monitoreo y validación final. Esta iniciativa refuerza la capacidad de defensa en estaciones de trabajo y servidores, incrementando la cobertura frente a amenazas avanzadas y aportando un marco de protección alineado con las mejores prácticas de seguridad.

Adicionalmente, se identificó que el Plan de Mejoramiento No 2396, orientado a fortalecer el control mediante escaneos semestrales de vulnerabilidades y pruebas de penetración a los sistemas de información, registraba hasta el 30 de junio de 2025 un avance del 0 % en la plataforma SIG. Lo anterior se debe a que la ejecución de las actividades inició apenas el 1 de abril de 2025 y los entregables son de carácter semestral; sin embargo, dada la criticidad del riesgo, resulta fundamental que la Oficina de Tecnología y Sistemas de Información (OTSI) acelere la ejecución y reporte de avances parciales que permitan verificar la trazabilidad de las acciones, más allá de esperar a la consolidación de informes semestrales.

Del análisis integral se concluye que, si bien el riesgo de corrupción no se materializó en el periodo evaluado, la magnitud de las vulnerabilidades detectadas y la deficiente trazabilidad en su gestión mantienen un riesgo residual alto. Esta situación demanda acciones correctivas orientadas a incrementar la efectividad de la remediación técnica, fortalecer los procesos de actualización tecnológica y garantizar la evidencia documental del cierre de vulnerabilidades.

III. COMPONENTE DE PLANEACIÓN Y FINANCIERA (PRESUPUESTO, PLANES, PROGRAMAS, PROYECTOS E INDICADORES)

En el marco de la revisión efectuada por esta auditoría, se verificaron las asignaciones presupuestales de la Oficina de tecnología y Sistemas de Información, de los compromisos adquiridos, los pagos realizados, la constitución de Cuentas por Pagar y Reservas a 31 de Diciembre de 2024, según se detalla en los siguientes cuadros**:**

EJECUCIÓN PRESUPUESTAL A 31 DE DICIEMBRE 2024

APR, VIGENTE	CDP	COMPROMISO	OBLIGACION	ORDEN PAGO	PAGOS	Reserva /Cuenta por pagar
2.471.677.481	2.471.677.481	2.471.677.481	1.695.454.669	1.695.454.669	1.695.454.669	776.222.812
32.263.353.157	32.213.996.082	32.213.996.082	16.881.419.471	16.783.829.989	16.783.829.989	15.332.576.611
1.000.000.000	1.000.000.000	1.000.000.000	0	0	0	1.000.000.000
149.937.521	149.937.521	149.937.521	0	0	0	149.937.521
2.919.944.003	2.919.944.003	2.919.944.003	38.102.610	38.102.610	38.102.610	2.881.841.393
1.752.002.063	1.748.213.738	1.748.213.738	1.404.994.485	1.404.994.485	1.404.994.485	343.219.254
600.000.000	600.000.000	600.000.000	600.000.000	600.000.000	600.000.000	0

APR, VIGENTE	CDP	COMPROMISO	OBLIGACION	ORDEN PAGO	PAGOS	Reserva /Cuenta por pagar
759.695.323	759.695.323	759.695.323	0	0	0	759.695.323
17.295.550.735	17.295.550.735	17.295.550.735	14.824.566.482	14.824.566.482	14.824.566.482	2.470.984.254
59.212.160.283	**59.159.014.883**	**59.159.014.883**	**35.444.537.716**	**35.346.948.234**	**35.346.948.234**	**23.714.477.167**

Fuente: Elaboración Propia -Oficina de tecnología y Sistemas de Información

La ejecución presupuestal de la Oficina de tecnología y Sistemas de Información durante el año 2024 se situó en un 59.70% sobre los pagos.

Por lo anterior, la OTSI informó "*que Las Cuentas fueron radicadas y no se pagó por disponibilidad de PAC de diciembre.*" constituyendo Cuentas Por Pagar y Reservas en un 40.09% equivalentes a **$23.714** millones.

CUENTAS POR PAGAR Y RESERVAS A DICIEMBRE 31-2024

Durante la revisión de las Reservas Constituidas por $23.714 millones por la OTSI para el año 2025, Están se desagregaron de la siguiente forma:

Para Cuentas por Pagar por $17.072. millones y Reservas por $6.642 millones. según se detalla en los siguientes cuadros:

CUENTAS POR PAGAR A 31 DE DICIEMBRE-2024

Dependencia	Dependencia Descripción	Identificación	Nombre Razón Social	VALOR
1700	OFIC. TECNOG	900105979	BMIND S.A.S. BIC	$ 380.817.700,00
1700	OFIC. TECNOG	800058607	CONTROLES EMPRESARIALES S A S	$ 1.233.058.646,23
1700	OFIC. TECNOG	830122983	ESRI COLOMBIA SAS	$ 30.408.000,00
1700	OFIC. TECNOG	900420814	HITSS COLOMBIA S.A.S	$ 598.954.372,00
1700	OFIC. TECNOG	830062674	INFORMACION LOCALIZADA S.A.S.	$ 268.932.573,62
1700	OFIC. TECNOG	900068796	INFOTIC S.A.	$ 14.522.348.525,00
1700	OFIC. TECNOG	900379439	TMS CORPORATION S.A.S	$ 37.877.369,00
TOTAL				**$ 17.072.397.185.85**

Fuente: Elaboración Propia -Oficina de tecnología y Sistemas de Información

Al 30 de Junio de 2025 estas cuentas ya están canceladas

RESERVAS A 31 DE DICIEMBRE -2024

IDENTIFICACION	NOMBRE RAZON SOCIAL	V/R. RESERVA
900068796	INFOTIC S.A.	$ 122.390.538,00
800167494	ADA S.A.S.	$ 895.028.869,00
800198591	BRANCH OF MICROSOFT COLOMBIA INC	$ 1.307.230.381,90
830126645	BUSINESS INTELLIGENCE SOFTWARE ASSESSOR CORPORATION S.A.S. BIC	$ 269.792.460,00
800058607	CONTROLES EMPRESARIALES S A S	$ 648.309.950,00
819006966	MEDIA COMMERCE PARTNERS S A S	$ 216.735.943,00
1019071855	ROZO BOLIVAR JAIME ANDRES	$ 9.145.000,00
800071819	SELCOMP INGENIERIA S.A.S. (SISTEMAS Y ELECTRONICA DE COMPUTADORES)	$ 357.137.418,00
900639534	SISELCOM SISTEMAS ELECTRICOS Y DE COMUNICACIONES SAS	$ 807.933.503,00
901661413	UNIÓN TEMPORAL INTERNEXA EN LA NUBE PRIVADA IV	$ 2.008.375.918,41
TOTAL		**$ 6.642.079.981,31**

Fuente: Elaboración Propia -Oficina de Tecnología y Sistemas de Información

Del total de las Reservas Constituidas de la OTSI a 31 de Diciembre de 2024 a Junio 30-2025, se han ejecutado el 73.67% equivalente a $4.482 millones, faltando por ejecutar el 26.33% es decir $1.749. millones, dentro del cual está el contrato ADA S.A.S. por valor de $895 millones. representando el 51.17% del total del saldo por ejecutar y un saldo para liberar del INFOTIC. de $122.millones entre otros.

Así mismo, la OTSI informo que el ***"contratista ADA. En la ejecución financiera a 30 de junio-2025……:*** *A la fecha del 30 de junio de 2025, del total de la reserva constituida no se ha pagado parte o la totalidad de este. De acuerdo con lo conversado, le confirmo que la forma de pago del contrato para productos de cumplen con todo el ciclo de la ingeniería de software, se pagan contra producto "terminado y aprobado de software". Razón por la cual, si bien hay avances en el ciclo de ingeniería de construcción de software, no se reflejan en el componente financiero por la forma de pago establecida en el contrato".*

Igualmente, para el contratista" INFOTIC la ejecución financiera a 30 de junio-2025…… *En el archivo enviado 3. Ejecución 2025, se puede evidenciar que la ejecución del saldo del compromiso a la fecha referida es de $14.644.739.063, quedando un saldo por $ 122.390.538,00 para liberar contra liquidación del contrato"*

En el siguiente cuadro se puede evidenciar el saldo pendiente a cancelar al 30 de junio de 2025, del total de las Reservas Constituidas y Cuentas por Pagar a 31 de diciembre de 2024.

RELACION DE LAS RESERVAS PENDIENTES DE CANCELAR AL 30 DE JUNIO-2025

Dependencia	Dependencia descripción	Identificación	Nombre Razón Social	Saldo por Utilizar en el RP a 31/12/2024	Saldo por Utilizar en el RP a 30/06/2025
1700	OFIC. TECNOL	800167494	ADA S.A.S.	$ 250.178.556,00	$ 250.178.556,00
1700	OFIC. TECNOL	800167494	ADA S.A.S.	$ 644.850.313,00	$ 644.850.313,00
1700	OFIC. TECNOL	900105979	BMIND S.A.S. BIC	$ 380.817.700,00	$ 0,00

Dependencia	Dependencia descripción	Identificación	Nombre Razón Social	Saldo por Utilizar en el RP a 31/12/2024	Saldo por Utilizar en el RP a 30/06/2025
1700	OFIC. TECNOL	800198591	BRANCH OF MICROSOFT COLOMBIA INC	$ 1.307.230.381,90	$ 0,00
1700	OFIC. TECNOL	830126645	BUSINESS INTELLIGENCE SOFTWARE ASSESSOR CORPORATION S.A.S. BIC	$ 269.792.460,00	$ 269.792.460,00
1700	OFIC. TECNOL	800058607	CONTROLES EMPRESARIALES S A S	$ 1.233.058.646,43	$ 0,00
1700	OFIC. TECNOL	800058607	CONTROLES EMPRESARIALES S A S	$ 648.309.950,00	$ 316.607.371,00
1700	OFIC. TECNOL	830122983	ESRI COLOMBIA SAS	$ 30.408.000,00	$ 0,00
1700	OFIC. TECNOL	900420814	HITSS COLOMBIA S.A.S	$ 598.954.372,00	$ 0,00
1700	OFIC. TECNOL	830062674	INFORMACION LOCALIZADA S.A.S.	$ 268.932.573,62	$ 0,00
1700	OFIC. TECNOL	900068796	INFOTIC S.A.	$ 14.644.739.063,00	$ 122.390.538,00
1700	OFIC. TECNOL	819006966	MEDIA COMMERCE PARTNERS S A S	$ 3.364.725,50	$ 3.364.725,50
1700	OFIC. TECNOL	819006966	MEDIA COMMERCE PARTNERS S A S	$ 213.371.217,50	$ 141.925.974,50
1700	OFIC. TECNOL	1019071855	ROZO BOLIVAR JAIME ANDRES	$ 9.145.000,00	$ 0,00
1700	OFIC. TECNOL	800071819	SELCOMP INGENIERIA S.A.S. (SISTEMAS Y ELECTRONICA DE COMPUTADORES)	$ 275.723.995,00	$ 0,00
1700	OFIC. TECNOL	800071819	SELCOMP INGENIERIA S.A.S. (SISTEMAS Y ELECTRONICA DE COMPUTADORES)	$ 25.133.168,00	$ 0,00
1700	OFIC. TECNOL	800071819	SELCOMP INGENIERIA S.A.S. (SISTEMAS Y ELECTRONICA DE COMPUTADORES)	$ 56.280.255,00	$ 0,00
1700	OFIC. TECNOL	900639534	SISELCOM SISTEMAS ELECTRICOS Y DE	$ 807.933.503,00	$ 0,00

Dependencia	Dependencia descripción	Identificación	Nombre Razón Social COMUNICACIONES SAS	Saldo por Utilizar en el RP a 31/12/2024	Saldo por Utilizar en el RP a 30/06/2025
1700	OFIC. TECNOL	900379439	TMS CORPORATION S.A.S	$ 37.877.369,00	$ 0,00
1700	OFIC. TECNOL	901661413	UNIÓN TEMPORAL INTERNEXA EN LA NUBE PRIVADA IV	$ 2.008.375.918,41	$ 0,00
TOTAL				**$ 23.714.477.167,36**	**$ 1.749.109.938,00**

Fuente: Elaboración Propia -Oficina de Tecnologia y Servicios

VIGENCIA 2025

Se llevó a cabo una revisión de la ejecución presupuestal de la Oficina de Tecnologia y Sistemas de Información con corte al 30 de Junio-2025. validando los compromisos adquiridos, los pagos realizados y el porcentaje de ejecución por rubros así:

EJECUCIÓN PRESUPUESTAL AL 30 DE JUNIO 2025

APR, VIGENTE	CDP	COMPROMISO	OBLIGACION	ORDEN PAGO	PAGOS
15.921.094.816	15.921.094.816	15.791.094.816	5.162.135.622	5.162.135.622	5.162.135.622
4.250.193.059	445.616.925	0	0	0	0
93.233.525	0		0	0	0
450.000.000	0		0	0	0
1.721.304.738	1.075.642.984	1.075.642.984	556.947.778	556.947.778	556.947.778
2.324.441.450	2.324.441.450	2.013.770.606	0	0	0
339.070.612	0		0	0	0
3.264.428.437	1.782.501.200	894.893.094	894.893.094	894.893.094	894.893.094
937.513.221	555.134.628	502.125.887	0	0	0
298.933.772	0		0	0	0
19.096.060.969	14.816.432.625	8.971.299.523	3.938.609.884	3.797.227.913	3.797.227.913
350.121.612	350.121.612	328.922.956	165.765.720	165.765.720	165.765.720
49.046.396.211	**37.270.986.240**	**29.577.749.866**	**10.718.352.098**	**10.576.970.127**	**10.576.970.127**

Fuente: Elaboración Propia -Oficina de Tecnologia y Sistemas de Información

El presupuesto apropiado para la vigencia 2025 de la Oficina de Tecnologia y Sistemas de Información es de $ 49.046 millones de los cuales al 30 de junio -2025, el 60.31% se han comprometido es decir $29.577 millones y pagados el 21.57% equivalente a $10.576 millones Evidenciándose una ejecución Presupuestal de un 21.57%, frente a los Pagos efectuados significativamente por debajo del 50% esperado por principio de anualidad. Esta baja ejecución

incluye rubros de contratos con un 0%. Por lo anterior, se urge implementar acciones de mejora para optimizar el desempeño presupuestal.

INDICADORES:

En el marco del seguimiento a la Oficina de Tecnologías y Sistemas de Información, se revisó los indicadores estratégicos definidos para las vigencias 2024 y 2025, con el propósito de evaluar el nivel de cumplimiento de las metas institucionales y la efectividad de los mecanismos de medición.

El análisis se orientó a verificar los avances en la implementación de acciones de gobierno y transformación digital, en la gestión de la conectividad escolar y en el monitoreo del rendimiento de las aplicaciones institucionales, con el fin de establecer si los resultados reportados reflejan una gestión eficiente, oportuna y alineada con los objetivos estratégicos de la entidad:

INDICADOR	REPORTES	OBSERVACIÓN OCI
Nombre: Eficiencia en las acciones de gobierno y transformación digital Tipo de acumulación: Mantenimiento Fórmula de cálculo: (Cantidad de acciones de transformación digital ejecutadas /Total de acciones planeadas) *100 Unidad de medida: Porcentaje Periodicidad: Trimestral	Para el periodo de 2024: El indicador se midió de forma acumulativa trimestral con una meta del 90 %, la cual se alcanzó en diciembre del 2024. Se ejecutaron iniciativas priorizadas en analítica geoespacial con la activación de ArcGIS Pro y tablero de control, automatización y robotización de procesos con avances en CRM y casos de uso, analítica predictiva y descriptiva con tableros y pruebas de ChatBot, y fortalecimiento de la red de líderes TIC con la elaboración del PETI y capacitaciones.	El indicador alcanzó la meta prevista de manera satisfactoria del 90%, reflejando un cumplimiento total en los compromisos de transformación digital establecidos para 2024. Se evidencia una gestión efectiva en el despliegue de proyectos estratégicos y una capacidad de articulación entre la Oficina de Tecnología y Sistemas de Información y las áreas funcionales involucradas.

Meta: 90%	El avance cuantitativo al segundo trimestre de 2025 alcanzó el 50 % de la meta programada para la vigencia. Se consolidaron iniciativas de transformación digital, destacándose la participación en mesas técnicas intersectoriales para fortalecer la analítica geoespacial, la gestión para la renovación de licenciamiento y continuidad en la automatización de procesos y robotización vinculados al POAIV y Asistencia Técnica, así como la definición de la arquitectura de referencia para la analítica descriptiva, predictiva y prescriptiva que permitirá integrar información de distintos sistemas bajo criterios de neutralidad tecnológica y mejor gobernanza de datos. No se reportaron cuellos de botella ni restricciones.	El resultado alcanzado es favorable, ya que evidencia un progreso constante en la implementación de las iniciativas priorizadas, mostrando compromiso institucional, articulación con áreas involucradas y una orientación técnica que impulsa la transformación digital en el sector educativo. La proyección lograda al segundo trimestre del 50 % permite inferir que el cumplimiento de la meta anual es viable si se mantiene la dinámica de trabajo demostrada

INDICADOR	REPORTES	OBSERVACIÓN OCI
Nombre: Eficiencia en la gestión de conectividad escolar Tipo de acumulación: Mantenimiento	Al cierre de la vigencia 2024 se alcanzaron 71 Secretarías de Educación Certificadas con proyectos de conectividad escolar viabilizados, lo que representó un avance cercano a la meta establecida del 74%. Se recibieron 162 proyectos de 89 secretarías, de los cuales se emitió concepto técnico para la totalidad. Dentro de los resultados, 80 obtuvieron viabilidad favorable, 77 no fueron favorables y 5 fueron cancelados por las mismas entidades. Se identificó que 26 secretarías no lograron viabilidad: 3 no presentaron proyectos, 4 no realizaron ajustes a las	El resultado del 74% muestra un esfuerzo de revisión exhaustiva y acompañamiento integral que permitió alcanzar un nivel alto de proyectos viabilizados. No obstante, la gestión se vio afectada por la falta de respuesta oportuna de algunas secretarías y por contrataciones realizadas sin concepto previo, lo que genera riesgos de control y limita el cumplimiento pleno de los objetivos

Fórmula de cálculo: (Cantidad de secretarias con proyectos viabilizados / Total de Secretarias de Educación Certificadas) *100 Unidad de medida: Porcentaje Periodicidad: Trimestral Meta: 74%	observaciones, y 19 contrataron sin autorización previa de la Oficina de Tecnología y Sistemas de Información, reduciendo así el universo de proyectos con concepto favorable.	de conectividad escolar. Se recomienda fortalecer los mecanismos de acompañamiento y supervisión para prevenir estas prácticas y mejorar la oportunidad en los ajustes solicitados.
	Durante el primer semestre del 2025 se alcanzó un total de 59 secretarías con proyectos viabilizados, lo que representa el 52% de cumplimiento frente a la meta intermedia definida para este periodo. En total se recibieron 86 proyectos provenientes de 69 secretarías, de los cuales 79 fueron revisados y emitidos conceptos técnicos para 67 secretarías. Los resultados muestran que 62 obtuvieron viabilidad favorable, 17 recibieron observaciones técnicas y 1 proyecto fue cancelado por la entidad proponente.	El avance refleja un cumplimiento adecuado del 52% respecto de la meta, lo que muestra mejoras en la agilidad y eficacia del proceso frente a periodos anteriores. Sin embargo, se evidenció una reducción en el número de proyectos viabilizados en comparación con el cierre de 2024, situación que responde a la disminución de propuestas recibidas y al estado pendiente de varios proyectos en revisión o ajuste. Se recomienda priorizar el acompañamiento a las 23 secretarías que no han presentado proyectos, a las 2 que se encuentran en revisión y a las 6 que están realizando ajustes, con el fin de fortalecer la cobertura y asegurar el cumplimiento de la meta anual.

INDICADOR	REPORTES	OBSERVACIÓN OCI
Nombre: Monitoreo del Rendimiento de Aplicaciones Tipo de acumulación: Mantenimiento Fórmula de cálculo: (Número de aplicaciones monitoreadas a través de APM /Total de aplicaciones priorizadas para monitorear a través de APM) *100 Unidad de medida: Porcentaje Periodicidad: Semestral Meta:100	El Ministerio de Educación Nacional avanzó en el monitoreo de ocho aplicaciones críticas: **SIMAT** (Sistema de Matriculas Estudiantil de Educación Básica y Media), **SIUCE** (Sistema de Información Unificado de Convivencia Escolar), **SIMPADE** (Sistema de Información para el Monitoreo, la Prevención y el Análisis de la Deserción Escolar), **SIFSE** (Sistema de Información de Fondos de Servicios Educativos), **SIET** (Sistema de Información de la Educación para el Trabajo y el Desarrollo Humano), **CEBYM** (Convalidaciones de Educación Básica y Media), **NEON** (Software para Gestión del Proceso Contractual) y **SSDIPI** (Sistema de Seguimiento al Desarrollo Integral de la Primera Infancia). Este seguimiento permitió identificar y supervisar el comportamiento de los sistemas en su operación diaria, facilitando la gestión institucional y el soporte a los procesos estratégicos del sector educativo.	El indicador alcanzó un desempeño adecuado del 100% al cubrir la totalidad de las aplicaciones priorizadas, lo que permitió mantener la continuidad y estabilidad de los servicios. Se destaca el aporte del monitoreo en la identificación de comportamientos y tendencias que fortalecen la gestión preventiva sobre los sistemas. Sin embargo, se recomienda optimizar los tiempos de adecuación de la infraestructura para garantizar que futuros despliegues o ampliaciones de monitoreo no enfrenten demoras.
	Durante el primer semestre de 2025, el monitoreo se concentró en dos aplicaciones: Sanción Mora y SIFSE, ambas con un rendimiento general óptimo. Se evidenció estabilidad y disponibilidad del 100%, sin registro de errores críticos en las transacciones. En Sanción Mora se identificaron tres anomalías leves y en SIFSE una única anomalía, ninguna con impacto significativo en la experiencia del usuario. El proceso se ejecutó sin dificultades ni restricciones.	El indicador mostró un cumplimiento pleno respecto a las aplicaciones priorizadas del 50% para el semestre, con resultados sobresalientes en términos de estabilidad y rendimiento. La estrategia de focalizar el monitoreo en sistemas específicos permitió un control detallado y efectivo. No obstante, es recomendable ampliar progresivamente el alcance hacia un mayor número de aplicaciones críticas para asegurar un cubrimiento total y mantener la meta del 100% establecida en el plan anual.

Fuente: Informe Indicadores - Subdirección de Desarrollo Organizacional

Como resultado del seguimiento realizado por la Oficina de control Interno se evidencio que, en materia de transformación digital, se alcanzaron plenamente las metas establecidas para el periodo evaluado, consolidando proyectos estratégicos que reflejan no solo capacidad técnica, sino también una adecuada articulación institucional y un enfoque de sostenibilidad a largo plazo. Entre los logros más relevantes se encuentran la implementación de soluciones de analítica geoespacial, la automatización y robotización de procesos, así como el desarrollo de herramientas de analítica predictiva y descriptiva que fortalecen la gestión basada en datos. Estos avances demuestran una gestión planificada y coordinada que posiciona a la entidad como referente en innovación tecnológica dentro del sector educativo, garantizando además la continuidad de las iniciativas y su alineación con las políticas nacionales de gobierno digital.

El indicador de conectividad escolar se constató avances importantes en el número de secretarías con proyectos viabilizados, lo cual contribuye a ampliar el acceso a servicios digitales en las instituciones educativas. Sin embargo, persisten limitaciones asociadas a secretarías que no presentan proyectos, que no realizan los ajustes técnicos solicitados o que avanzan en contrataciones sin contar con concepto previo de viabilidad. Estas situaciones generan riesgos de control, reducen la cobertura efectiva y pueden comprometer el cumplimiento de la meta anual definida. A pesar de ello, la gestión muestra mejoras en los tiempos de revisión y en la calidad del acompañamiento brindado, lo que representa una oportunidad para consolidar los avances si se fortalecen los mecanismos de supervisión y asistencia técnica.

Por su parte, el monitoreo del rendimiento de aplicaciones confirma niveles sobresalientes de estabilidad y disponibilidad en los sistemas priorizados, con indicadores que alcanzan hasta el 100 % y sin afectaciones significativas para los usuarios. Este resultado demuestra la eficacia de las herramientas de monitoreo aplicadas y la capacidad preventiva de la entidad para anticipar anomalías y garantizar la continuidad de los servicios. No obstante, el alcance reducido del monitoreo —limitado a un conjunto específico de aplicaciones críticas— impide contar con una visión integral del desempeño de toda la infraestructura tecnológica. Esta limitación constituye un riesgo, ya que la falta de cobertura amplia puede dificultar la detección temprana de fallas o vulnerabilidades en otros sistemas que también son esenciales para la operación institucional.

IV. COMPONENTE DE CONTRATACIÓN (EVALUACIÓN DE CONTRATOS)

De acuerdo con la relación de contratos de la Oficina de Tecnologías y Sistemas de Información (OTSI) correspondientes a las vigencias 2024 y 2025, periodo objeto de auditoría, se tomó como base la totalidad de los contratos asociados al Proceso de Gestión de Servicios TIC, donde se revisó la contratación con énfasis en el cumplimiento de los perfiles del personal técnico exigido y en la ejecución contractual vinculada.

Para este propósito, se seleccionó una muestra de doce (12) contratos, validando en la plataforma SECOP II la documentación requerida durante la ejecución de los siguientes contratos observando lo siguiente:

En las asignaciones de usuarios que son los trámites que se otorgan para el trabajo del contratista, es claro de que la exigencia del pantallazo del SGDEA en el informe de ejecución es válida y cuenta como soporte, verificando las respuestas oportunas a cada comunicación teniendo así un control. Como lo establece el manual de supervisión CN-MA-02 en su versión 2, donde dice que el contratista "cumpla las directrices implementadas en el SGD, para el manejo integral de la información y que atienda con la oportunidad debida los radicados que le sean asignados en el marco de la ejecución del objeto pactado, de modo que el respectivo aplicativo de correspondencia se mantenga actualizado y al día". Para qué el supervisor puede ejercer control sobre la ejecución contractual y el contratista dispone de evidencia suficiente de sus actuaciones.

CONTRATOS 2024:

TABLA 1. SEGUIMIENTO CONTRATO: CO1.PCCNTR.6716924

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.6716924	OSCAR ALFREDO FAJARDO ORTEGA	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.6648098&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES DE APOYO A LA SUPERVISIÓN EN LAS ACTIVIDADES DE GESTIÓN, SEGUIMIENTO Y CONTROL AL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN, MONITOREO Y PRUEBAS DE RECUPERACIÓN DE DESASTRES, DE ACUERDO CON LA NORMATIVIDAD VIGENTE

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	01/08/2024 - CDP $36.580.000 06/09/2024 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 7 Proyectar y/o revisar de manera oportuna (en los tiempos que establezca la herramienta dispuesta por el MEN) la correspondencia generada y recibida a través del Sistema de Gestión Documental o cualquier otro canal de notificación con los que cuente el Ministerio Se observo a satisfaccion los pagos con los soportes, como son las evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 2. SEGUIMIENTO CONTRATO: CO1.PCCNTR.6720432

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.6720432	FRANKLIN AUGUSTO PINTO CARREÑO	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.6652468&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA ORIENTAR EL DESARROLLO DE LAS FASES DE INGENIERÍA DE SOFTWARE Y BRINDAR SOPORTE TÉCNICO EN LOS PROYECTOS DE FORTALECIMIENTO DEL CICLO DE VIDA DEL ECOSISTEMA TI DE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	01/08/2024 - CDP $36.578.696 06/09/2024 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOPII se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. **III. Asignaciones en el Sistema de Gestión Documental:** Que el estado de mis asignaciones en el sistema de gestión documental es el siguiente: Estado / No. / Observación A tiempo Para vencerse Vencido Se observó que en los informes de los meses octubre, noviembre y diciembre 2024, quedando el "Estado de avance de la ejecución física a la fecha (%)" todos en un 25%, los soportes, como son las evidencias, pago de seguridad social y certificados de satisfacción del supervisor se encuentran debidamente cargados y firmados.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 3. SEGUIMIENTO CONTRATO: CO1.PCCNTR.6410261

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.6410261	ANDRES FELIPE FORERO HUERTAS	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.6236315&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA ESTRUCTURAR EL HUB DE INFORMACIÓN DEL MINISTERIO DE EDUCACIÓN NACIONAL, DEFINIR POLÍTICAS Y ESTÁNDARES QUE PERMITAN APROVECHAR LOS DATOS, LA INFORMACIÓN Y EL CONOCIMIENTO GEOESPACIAL GENERADO DESDE LA ENTIDAD

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	20/05/2024 - CDP $64.012.718 07/06/2024 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOPII se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. **III. Asignaciones en el Sistema de Gestión Documental:** Que el estado de mis asignaciones en el sistema de gestión documental es el siguiente: Estado / No. / Observación A tiempo Para vencerse Vencido Se observó que en el informe del periodo mes de agosto, lo reportaron como julio 2024, los soportes, como son las evidencias, pago de seguridad social y certificados de satisfacción del supervisor se encuentran debidamente cargados y firmados.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

CONTRATOS 2025:

TABLA 4. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7217317

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7217317	VARGAS VILLEGAS FELIX FERNANDO	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7311068&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA ORIENTAR, ESTRUCTURAR Y HACER SEGUIMIENTO SOBRE LAS NECESIDADES DE LOS PROYECTOS DE FORTALECIMIENTO DE SOLUCIONES TECNOLÓGICAS DEL ECOSISTEMA DIGITAL DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	NO ESTA PUBLICADO LA DEPENDENCIA DEBE CARGAR EL DOCUMENTO SOPORTE	07/01/2025 - CDP $159.888.612 13/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 9 Solucionar y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se evidencia que no se encuentra cargado el contrato en la plataforma del SECOP II. Se observó a satisfacción los pagos con los soportes, como es el pago de seguridad social y certificados de satisfacción del supervisor, en las evidencias cargadas no especifican el objetivo de la actividad, solo pantallazos, se sugiere al supervisor realice una acción de control para los próximos informes, estos evidenciados desde el primero al cuarto informe de supervisión.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 5. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7212732

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7212732	CARVAJAL FERRER LUIS EDUARDO	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7303223&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA EL SEGUIMIENTO, FORTALECIMIENTO Y GESTIÓN DEL CICLO DE VIDA DEL ECOSISTEMA TI PRINCIPALMENTE DE SISTEMAS DE EDUCACIÓN SUPERIOR

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	07/01/2025 - CDP $132.884.916 12/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 9 Solucionar y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se observó a satisfacción los pagos con los soportes, como son las evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 6. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7268112

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7268112 CO1.PCCNTR.7971322	HANET MENDEZ LINARES	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7373615&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	**1, CO1.PCCNTR.7268112**: PRESTACIÓN DE SERVICIOS PROFESIONALES PARA APOYAR LA SUPERVISIÓN DEL CONTRATO CON LA FIDUPREVISORA PARA LAS OBLIGACIONES DE GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	09/01/2025 - CDP $101.995.018 17/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 7 Proyectar y/o revisar de manera oportuna la correspondencia generada y recibida a través del Sistema de Gestión Documental o cualquier otro canal de notificación con los que cuente el Ministerio. Se observó a satisfacción los pagos con los soportes, como son las evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 7. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7217310

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7217310	GAMBOA COMEZANA JOSE MAURICIO	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7311367&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA ORIENTAR EL DESARROLLO DE LAS FASES DE INGENIERÍA DE SOFTWARE Y BRINDAR SOPORTE TÉCNICO EN LOS PROYECTOS DE FORTALECIMIENTO DEL CICLO DE VIDA DEL ECOSISTEMA TI DE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	NO ESTA PUBLICADO LA DEPENDENCIA DEBE CARGAR EL DOCUMENTO SOPORTE	08/01/2025 - CDP $115.552.104 12/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 11 Solucionar y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se evidencia que no se encuentra cargado el contrato en la plataforma del SECOP II. Se observó a satisfacción los pagos con los soportes, evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 8. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7244103

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7244103	FORERO HUERTAS ANDRES FELIPE	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7346683&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA ESTRUCTURAR EL HUB DE INFORMACIÓN DEL MINISTERIO DE EDUCACIÓN NACIONAL, DEFINIR POLÍTICAS Y ESTÁNDARES QUE PERMITAN APROVECHAR LOS DATOS, LA INFORMACIÓN Y EL CONOCIMIENTO GEOESPACIAL GENERADO DESDE LA ENTIDAD.

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	09/01/2025 - CDP $110.737.433 17/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. **III. Asignaciones en el Sistema de Gestión Documental:** Que el estado de mis asignaciones en el sistema de gestión documental es el siguiente: Estado / No. / Observación A tiempo / N.A. / N.A. Para vencerse / N.A. / N.A. Vencido / N.A. / N.A. Se observó a satisfacción los pagos con los soportes, evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 9. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7215642

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7215642	YINI PAOLA LEIVA NARANJO	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7303289&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA BRINDAR SOPORTE, GESTIÓN TÉCNICA E INGENIERÍA DE SOFTWARE SOBRE LOS SISTEMAS DE INFORMACIÓN NUEVOS Y EXISTENTES DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	07/01/2025 - CDP $106.429.584 13/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 9 — Solucionar y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se observó a satisfacción los pagos con los soportes, evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 10. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7212393

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7212393	HAROLD YESID PERDOMO FALLA	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7303797&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA ORIENTAR, ESTRUCTURAR Y HACER SEGUIMIENTO SOBRE LAS NECESIDADES DE LOS PROYECTOS DE FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DIGITAL Y SEGURIDAD INFORMÁTICA DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	70/01/2025 - CDP $159.888.612 11/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 9 Solucionar y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se observó a satisfacción los pagos con los soportes, evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 11. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7248330

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7248330	BERNAL MURCIA EDWIN ALEXANDER	community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7348567&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA BRINDAR SOPORTE Y GESTIÓN TÉCNICA DE LOS PROYECTOS DE FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DIGITAL DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	09/01/2025 - CDP $52.961.381 17/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 7 Solucionar con análisis de causa raíz y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se observó a satisfacción los pagos con los soportes, evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

TABLA 12. SEGUIMIENTO CONTRATO: CO1.PCCNTR.7261122

CONTRATO	CONTRATISTA	LINK CONSULTA PUBLICA	MODALIDAD DE CONTRATACIÒN CORRECTAMENTE SELECCIONADA	OBJETO DEL CONTRATO
CO1.PCCNTR.7261122	IVAN LEONARDO AGUASACO GONZALEZ	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7365565&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATACIÓN DIRECTA	PRESTACIÓN DE SERVICIOS PROFESIONALES PARA BRINDAR SOPORTE TÉCNICO DE LOS PROYECTOS DE FORTALECIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DIGITAL DEL MINISTERIO

ESTUDIOS PREVIOS DISPONIBLES Y PUBLICADOS	CONTRATO DEBIDAMENTE CARGADO EN SECOP II	REGISTRO PRESUPUESTAL (CDP/RP) ANEXADO	EXPERIENCIA	OBSERVACIONES OCI
ESTUDIO PREVIO PUBLICADO	CONTRATO PUBLICADO	09/01/2025 - CDP $41.797.256 28/01/2025 - RP	CUMPLE	En la verificación del contrato en la plataforma SECOP II, se tiene la posibilidad de ingresar a los soportes de consulta pública, observándose el no cargue del pantallazo del SGDEA. 7 Solucionar con análisis de causa raíz y cerrar dentro del término del Acuerdo de Nivel de Servicio (ANS) los casos de servicios de TI asignados a través de la mesa de servicio, Sistema de Gestión documental y el correo electrónico. Se observó a satisfacción los pagos con los soportes, evidencias, pago de seguridad social y certificados de satisfacción del supervisor.

Fuente: SECOP II-Elaboración propia de la Oficina de Control Interno

La revisión contractual de los perfiles técnicos permitió concluir que se cumplió con la experiencia exigida en los estudios previos, lo que garantiza que los profesionales vinculados contaran con la idoneidad necesaria para el desarrollo de las actividades contratadas y que la ejecución contractual se respaldara en capacidades técnicas adecuadas para atender los requerimientos del Proceso de Gestión de Servicios TIC.

No obstante, también se identificaron situaciones que requieren atención, pues en algunos contratos se evidenció que los informes de avance permanecieron estáticos durante varios meses sin reflejar de manera precisa la evolución de las actividades, como ocurrió con el contrato de apoyo en ingeniería de software que reportó un avance del 25 % en los tres últimos cortes del año, lo que limita la utilidad de los informes como herramienta de control y seguimiento y debilita la oportunidad en la información presentada.

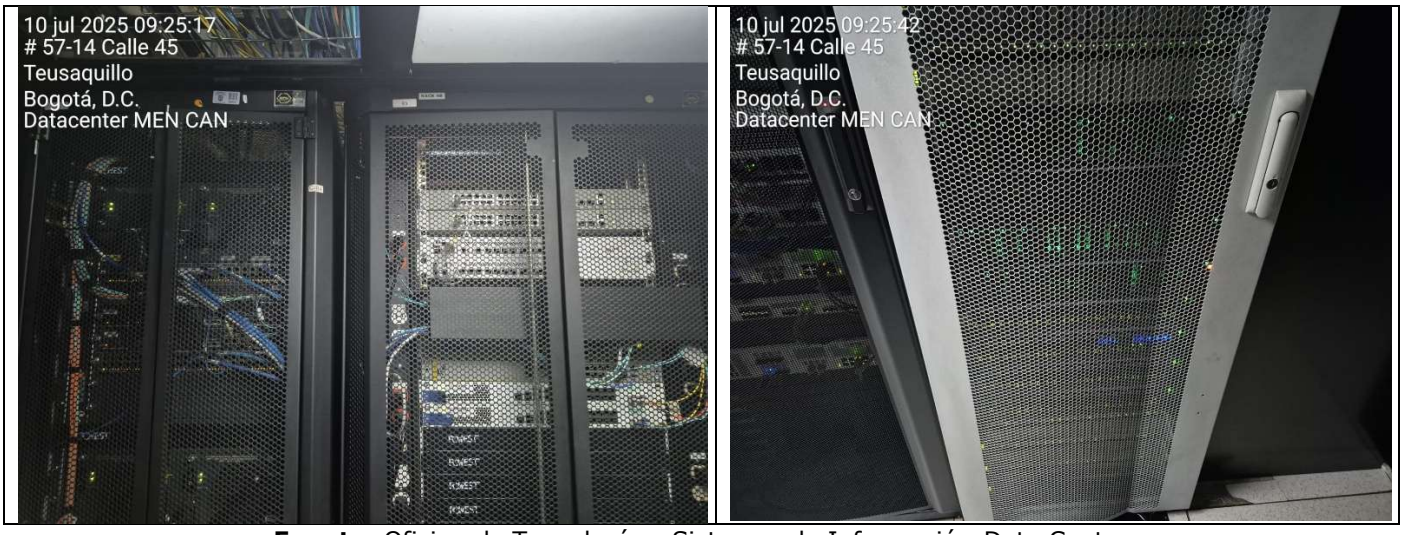
Asimismo, se detectaron inconsistencias en la denominación de los periodos de seguimiento, como el caso de un informe correspondiente a agosto que fue registrado como si perteneciera a julio, lo que pone de manifiesto falencias en la disciplina de reporte y afecta la confiabilidad de la información utilizada para el control contractual.

V. COMPONENTE TECNOLÓGICO

Con el propósito de realizar seguimiento a los controles del Anexo de la 27001:2022, se adelantó la revisión encaminada en la verificación de la eficacia de las medidas implementadas para proteger la infraestructura crítica, asegurar la continuidad de los servicios y garantizar la integridad de la información. Este ejercicio contempló la evaluación de controles asociados a la seguridad física del datacenter, la gestión de cambios y configuraciones, los procesos de respaldo y restauración, así como la disposición ambientalmente responsable de materiales y equipos al final de su vida útil.

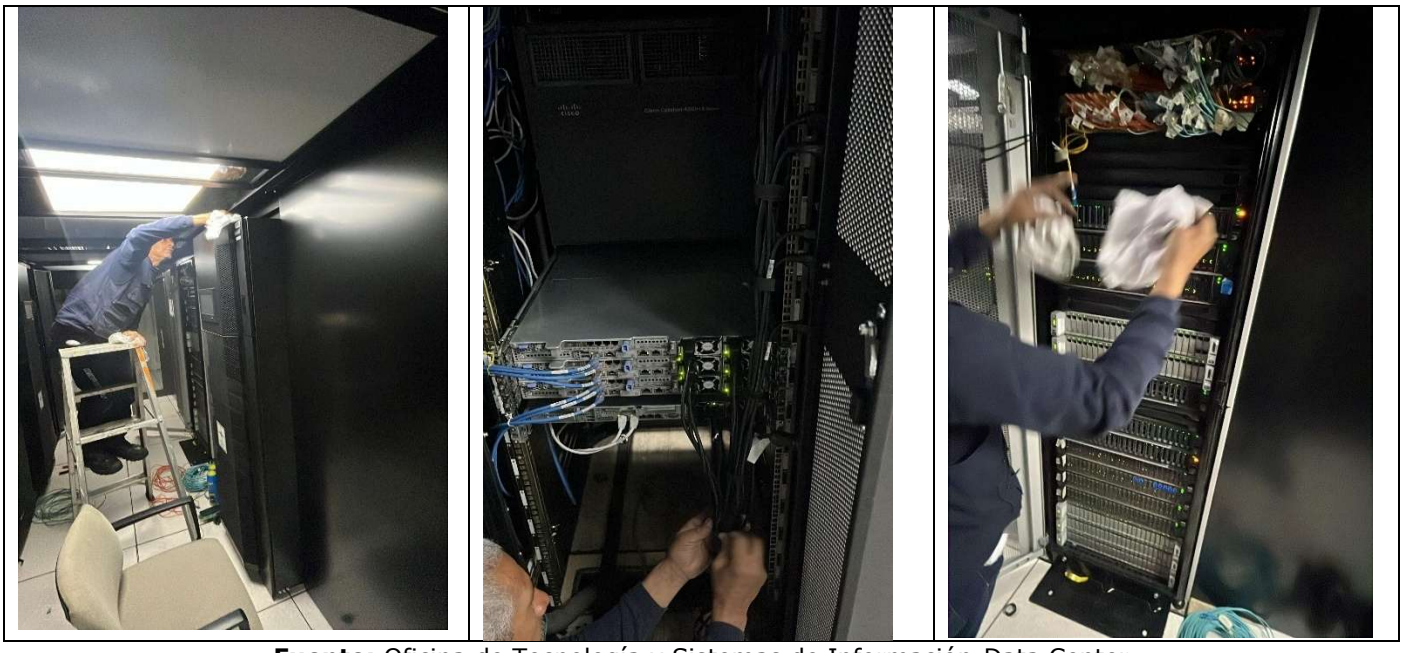
A) SEGURIDAD FÍSICA Y CONTINUIDAD OPERATIVA:

El Ministerio de Educación Nacional dispone de un sistema de climatización especializado mediante aires acondicionados de precisión, diseñados específicamente para entornos de misión crítica como los centros de datos, lo cual permite mantener de forma constante la temperatura y la humedad relativa en los rangos óptimos recomendados por los fabricantes de hardware.



Fuente: Oficina de Tecnología y Sistemas de Información-Data Center

Este control resulta esencial para preservar la vida útil de los equipos, evitar el sobrecalentamiento de servidores y dispositivos de red, así como prevenir la condensación que podría generar corrosión o fallas eléctricas. La existencia de un canal de fibra óptica dedicado que enlaza los datacenters garantiza, además, que los sistemas de respaldo y replicación funcionen en condiciones ambientales estables, incrementando la seguridad y la confiabilidad de las operaciones tecnológicas.



Fuente: Oficina de Tecnología y Sistemas de Información-Data Center

Adicionalmente, se ejecutan mantenimientos preventivos de manera semestral a racks, cableado estructurado y sistemas de energía, lo que asegura que la infraestructura soporte se conserve en condiciones óptimas y libre de riesgos asociados a desgaste o deterioro. Estos contemplan la inspección física de conexiones, la limpieza de componentes, la verificación de patch panels y la correcta distribución de cargas eléctricas en los equipos, acciones que contribuyen a mitigar puntos calientes y a prevenir fallas por interferencias electromagnéticas.

También, se revisó la renovación oportuna de baterías de las UPS a inicios de 2024, siguiendo la vida útil recomendada por el fabricante, y con un proceso de disposición final certificado que cumple con la normativa ambiental y las exigencias de la autoridad competente, evidenciando una clara articulación entre gestión tecnológica y responsabilidad ambiental.

Estos controles no solo aseguran la disponibilidad continua de la infraestructura tecnológica, sino que también fortalecen la resiliencia institucional frente a interrupciones derivadas de fallas eléctricas, ambientales o de deterioro de los equipos de soporte.

B) GESTIÓN DE CAMBIOS Y CONFIGURACIONES:

El control de cambios se gestiona a través de solicitudes formales (RFC) que son revisadas de manera estructurada por un comité especializado en el que participan responsables de infraestructura, aplicaciones y seguridad, lo que asegura un análisis integral antes de la autorización de cualquier modificación.

TABLA DE RFCS PARA APROBACIÓN POR COMITE

RFCs para aprobación

A continuación se relaciona el estado de las ordenes de cambios presentadas para evaluar en el comité de cambios del CAB No. 558 por parte de los frentes encargados de Infraestructura y Aplicaciones del Ministerio de Educación Nacional como se evidencia en la siguiente tabla, así:

Fecha Solicitud	Ticket	Estado	Descripción del Cambio	Solicitante / Líder Técnico	Ambiente
4/06/2025	OC97933	APROBADO	Crear copia de bases de datos y servidor de aplicaciones APP047 para entrega a la fábrica de software	EDNA AREVALO	Producción
4/06/2025	OC97927	APROBADO	Actualización Aria Operations for logs	MARIO LOPEZ	Producción
29/05/2025	OC97859	APROBADO	Se entregan recursos que no se usan para posteriormente ser usados en la fase 2 de PENSIONADOS Produccion	ALEXANDER NOVA	Certificación
30/05/2025	OC97862	APROBADO	Realizar actualización de la Data en ambiente de certificación para realizar las pruebas de los sistemas de información SIMAT y SINEB y que puedan sincronizar con la nueva data	JUAN PERILLA	Producción
3/06/2025	OC97924	APROBADO	Realizar mantenimiento preventivo y correctivo de puntos de red de datos y puntos de energía regulada de los puestos de trabajo del piso 1 Oriente y Occidente del MEN.	JAVIER RODRIGUEZ	Producción
30/05/2025	OC97885	APROBADO	Ambiente de certificación SIPTA- Restauración de la bd de producción en el ambiente de certificación del sistema SIPTA	WILSON ROMERO	Producción
3/06/2025	OC97925	APROBADO	Realizar el cambio de 2 Switch 2960x (Nuevos, Gestión Bajo RMA Cisco) correspondientes al STACK del piso 2 Oriente	JAVIER RODRIGUEZ	Producción

Fuente: Oficina de Tecnología y Sistemas de Información

Cada RFC es evaluada en función de los riesgos asociados, el impacto potencial en la disponibilidad de los servicios y la definición de ventanas de mantenimiento que permitan ejecutar los cambios de forma controlada, minimizando las afectaciones al ambiente productivo. Este procedimiento garantiza trazabilidad documental de principio a fin, desde la identificación de la necesidad del cambio hasta la verificación de su correcta implementación, reduciendo así la probabilidad de que se introduzcan alteraciones no autorizadas o que generen incidentes operativos.

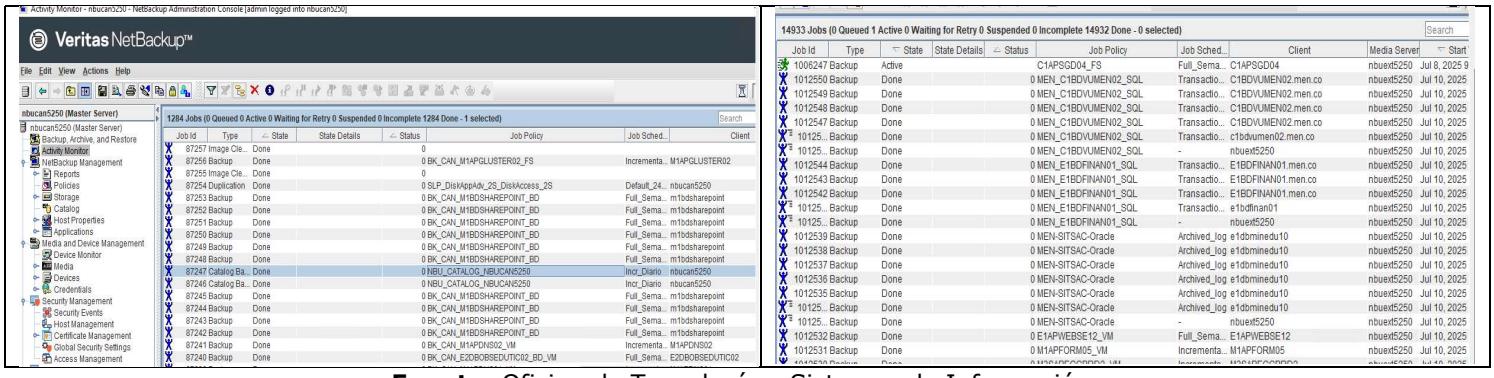
Aunque el equipo de infraestructura no administra directamente los servidores, se constató que los cambios significativos en bases de datos, plataformas de identidad y servicios de red se gestionan bajo el mismo esquema formal de autorización, lo que refleja coherencia y madurez en el proceso. Además, la existencia de actas de los comités de cambios respalda la transparencia y la rendición de cuentas, evidenciando que no todos los cambios son aprobados de manera automática, sino que se aplican criterios técnicos y de seguridad para rechazar aquellos que no cumplen con las condiciones establecidas o que requieren validaciones adicionales.

C) RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN:

El sistema de respaldo implementado presenta un diseño integral que combina diferentes frecuencias de ejecución: diaria, semanal, mensual y anual, lo que permite cubrir tanto la operación cotidiana como la conservación histórica de la información. Esta planificación de retención garantiza que la entidad pueda acceder a datos recientes para la recuperación rápida de incidentes menores, al tiempo que preserva copias de largo plazo para atender requerimientos o necesidades estratégicas de continuidad operativa.

El esquema cuenta con un modelo de redundancia robusta, soportado en datacenters espejo localizados en Bogotá y Tocancipá, lo cual asegura la replicación sincrónica y asincrónica de los respaldos. Esta arquitectura no solo minimiza el riesgo de pérdida de información en caso de contingencias, sino que también amplía la capacidad de recuperación frente a escenarios de desastre, aportando resiliencia y disponibilidad continua de los servicios críticos. La localización geográfica diferenciada de los centros de datos reduce la exposición y garantiza que la organización cumpla con las mejores prácticas de seguridad y continuidad del negocio.

PANTALLAZOS DEL SISTEMA DE BACKUP



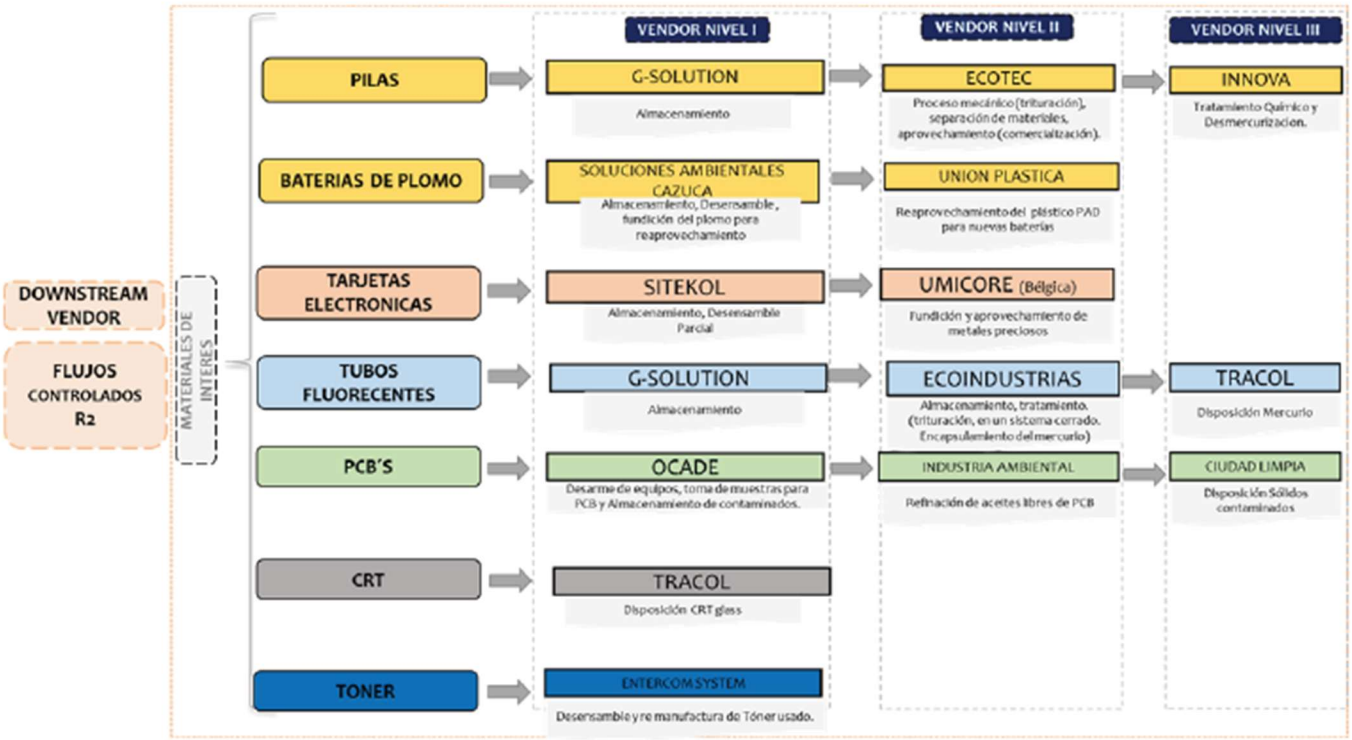
Fuente: Oficina de Tecnología y Sistemas de Información

Adicionalmente, la entidad dispone de un plan formal de pruebas de restauración, diseñado para verificar periódicamente la confiabilidad y usabilidad de los respaldos. Dicho plan contempla la ejecución programada de simulaciones bajo distintos escenarios de falla, cuyos resultados se documentan en informes técnicos ya validados. La evidencia recopilada demuestra que las copias de seguridad no solo existen, sino que son funcionales y efectivas en procesos de recuperación, asegurando así la integridad de la información.

D) GESTIÓN AMBIENTAL Y DISPOSICIÓN DE MATERIALES:

Mediante el Plan de Materiales de Interés, el Ministerio de Educación Nacional evidencia una adecuada gestión de equipos y residuos electrónicos, integrando criterios de sostenibilidad y cumplimiento normativo en la operación tecnológica. Este plan se encuentra alineado con estándares internacionales como la norma R2 y con compromisos adquiridos a través del Acuerdo de Minamata, garantizando que materiales peligrosos, en particular aquellos que contienen mercurio, sean manejados bajo procesos de separación, clasificación, almacenamiento temporal y disposición final realizados por gestores certificados, lo que asegura un tratamiento ambientalmente seguro y controlado.

CADENA DE DISPOSICIÓN RESIDUOS TECNOLOGICOS



Fuente: Pcshek Tecnología y servicios S.A.S.

La estrategia implementada no se limita al cumplimiento formal de la normativa, sino que incorpora prácticas de economía circular al priorizar la reutilización, el reacondicionamiento y el reciclaje de equipos antes de su disposición final, reduciendo la huella ambiental institucional y contribuyendo al aprovechamiento de materiales que aún son útiles. Esto representa una integración efectiva entre la gestión ambiental y la gestión tecnológica, consolidando un modelo operativo que protege tanto al entorno como a la infraestructura crítica.

De la misma manera, contemplan medidas específicas para la protección de los trabajadores que manipulan estos materiales, estableciendo el uso de elementos de protección personal, protocolos de higiene y controles de exposición que previenen riesgos en salud ocupacional y garantizan condiciones seguras en las labores de disposición. Este aspecto refleja una articulación positiva entre la gestión ambiental y la seguridad y salud en el trabajo, ampliando el alcance de los beneficios de su implementación.

VI. MANUALES, POLÍTICAS, PROCEDIMIENTOS, GUÍAS, PROTOCOLOS

1. Procedimientos de Gestión de Seguridad de la Información, ST-PR-08 – Versión 4:

El procedimiento ST-PR-08 versión 04 constituye una base sólida para la gestión de la seguridad de la información en el Ministerio de Educación Nacional ya que establece de manera clara como objetivo central la mejora continua del SGSI orientada a proteger la confidencialidad la integridad y la disponibilidad de los activos de información y esto lo convierte en un documento alineado con los principios rectores de la norma ISO/IEC 27001:2013 al dar prioridad a la preservación de los atributos esenciales de la información y a la continuidad institucional.

En cuanto a la documentación del procedimiento se concluye lo siguiente:
La definición del alcance es adecuada porque delimita de manera concreta el inicio con la realización del autodiagnóstico y el cierre con la formulación de planes de mejoramiento lo cual asegura un ciclo ordenado que permite planificar implementar y evaluar de forma periódica acciones de fortalecimiento del SGSI este enfoque muestra un compromiso institucional con el análisis de resultados y con la construcción de planes que generen valor al sistema y a los servicios educativos apoyados en las TIC.

Las disposiciones generales evidencian una integración acertada con el Sistema Integrado de Gestión ya que articulan políticas objetivos controles declaración de aplicabilidad y tratamiento de datos personales dentro de un marco documental único y centralizado esto garantiza coherencia institucional y facilita que los servidores y contratistas cuenten con directrices claras para el cumplimiento de la seguridad digital además se contempla la inspección anual liderada por la OTSI como una buena práctica para verificar la implementación de controles y reforzar la cultura de seguridad.

La parte descriptiva refleja una estructura que contempla once actividades que cubren todas las fases del ciclo de mejora desde el diagnóstico hasta la retroalimentación y dentro de estas actividades se destacan la gestión de activos, la gestión de riesgos, la gestión de incidentes, el

reporte de indicadores, la ejecución de planes y la revisión por la dirección lo cual demuestra un sistema que no se limita a la planeación sino que incorpora seguimiento auditoría interna y planes de mejoramiento lo que asegura continuidad y madurez en la gestión

La gestión de activos de información es un punto fuerte porque establece un mecanismo específico para clasificar y administrar los activos determinando roles responsabilidades y niveles de clasificación lo que contribuye a que la información sea utilizada de forma adecuada y a que cada funcionario conozca sus responsabilidades frente a los recursos de información esta práctica es coherente con los requisitos del Anexo A de la norma que exige control sobre activos y responsabilidades asociadas.

En la gestión de riesgos el procedimiento se apoya en guías institucionales oficiales y lineamientos estatales lo que fortalece la estandarización de metodologías y asegura que las decisiones se tomen con criterios homogéneos y validados a nivel gubernamental esta articulación garantiza que la valoración de riesgos esté alineada tanto con los objetivos de información del MEN como con directrices nacionales lo que refuerza la solidez del análisis y la adopción de medidas

El componente de gestión de incidentes es pertinente, porque asegura que la entidad cuente con un procedimiento formal para atender eventualidades que puedan afectar la confidencialidad la integridad o la disponibilidad de la información además establece como prioridad la pronta recuperación de los servicios TIC lo cual es esencial para garantizar la continuidad de la operación educativa y para mantener la confianza en la institución frente a usuarios internos y externos.

La incorporación de indicadores del SGSI promueve una práctica de gestión acertada ya que permite evaluar de manera objetiva los avances alcanzados y comparar resultados frente a metas definidas este enfoque de medición promueve la toma de decisiones basada en datos y asegura que la entidad cuente con evidencia objetiva para direccionar acciones de mejora y asignar recursos de manera estratégica fortaleciendo así la transparencia y la rendición de cuentas

El procedimiento también fortalece la ejecución y el monitoreo de los planes de seguridad ya que incluye no solo el plan de seguridad y privacidad y el plan de tratamiento de riesgos sino también la estrategia de concienciación y el plan de cierre de brechas esta amplitud de alcance demuestra un compromiso integral con la seguridad porque combina aspectos técnicos con factores humanos y organizacionales garantizando que la seguridad digital no sea solo un tema de controles sino también de cultura institucional.

La inclusión de auditorías internas y revisión por la dirección confirma que el procedimiento no se queda en el nivel operativo, sino que asciende al nivel estratégico con mecanismos de evaluación independiente y análisis directivo de la conveniencia la eficacia y la alineación del sistema lo que asegura que los resultados sean conocidos al más alto nivel y que se tomen decisiones informadas sobre recursos prioridades y oportunidades de mejora.

Finalmente, el cierre con la gestión de planes de mejoramiento evidencia un compromiso real con la retroalimentación del sistema ya que se garantiza que todos los hallazgos tanto internos como externos se conviertan en acciones verificables que fortalecen el desempeño institucional este enfoque asegura un ciclo virtuoso donde cada evaluación genera un aprendizaje y cada aprendizaje se transforma en una acción de mejora consolidando un SGSI robusto y en evolución constante.

2. Gestión de incidentes de seguridad de la información - ST-PR-18 – Versión 2.

El procedimiento ST-PR-18 versión 02 de gestión de incidentes de seguridad de la información es un documento bien diseñado que aporta valor al Sistema de Gestión de Seguridad de la Información del Ministerio de Educación Nacional porque establece un objetivo claro orientado a garantizar una atención eficaz y coordinada de los incidentes con el fin de minimizar impactos en la confidencialidad la integridad y la disponibilidad de los activos de información lo cual refleja coherencia con los principios de la norma ISO/IEC 27001:2022 y con las buenas prácticas internacionales de seguridad digital.

En cuanto a la documentación del procedimiento se concluye lo siguiente:

El alcance definido resulta positivo porque cubre de manera completa el ciclo de vida de los incidentes desde su detección y reporte hasta la documentación de lecciones aprendidas y la implementación de mejoras preventivas lo que asegura que la gestión no se limite a contener el incidente, sino que busque erradicar sus causas y prevenir recurrencias generando un proceso de aprendizaje organizacional que refuerza la madurez del SGSI

Las disposiciones generales son un punto fuerte porque establecen lineamientos claros de reporte atención y escalamiento incluyendo la obligación de registrar todos los incidentes en la herramienta de gestión CA Service Desk para garantizar trazabilidad y además definen la notificación temprana a ColCERT y CSIRT Gobierno dentro de las primeras 24 horas lo que demuestra alineación con los requerimientos nacionales de ciberseguridad y refuerza la cooperación interinstitucional en la respuesta a incidentes críticos.

El documento también evidencia un adecuado enfoque en la cadena de custodia y la preservación de evidencias lo cual es fundamental para garantizar validez en los procesos de investigación forense y para respaldar la toma de decisiones tanto técnicas como legales además se identifican roles responsabilidades y competencias necesarias para el personal lo que contribuye a asegurar que las actividades de respuesta sean ejecutadas por profesionales idóneos.

La matriz RACI es un elemento que clarifica de manera visual la asignación de responsabilidades en cada etapa del procedimiento y evita ambigüedades en la ejecución lo cual mejora la coordinación entre usuarios mesa de ayuda responsables de seguridad grupo de respuesta e instancias externas generando una dinámica de colaboración eficiente y estructurada.

La parte descriptiva del procedimiento constituye una fortaleza mayor ya que establece paso a paso dieciocho actividades que inician con el reporte y evaluación del incidente y culminan con el cierre formal y la documentación de lecciones aprendidas cada actividad cuenta con responsables tiempos máximos y evidencias lo que permite medir el desempeño asegurar cumplimiento oportuno y mantener trazabilidad completa sobre el manejo de los incidentes.

La perspectiva en contención erradicación y recuperación es adecuado porque garantiza que el incidente no solo sea detenido sino también corregido en sus causas y que los sistemas afectados se restauren a la normalidad con la menor afectación posible además se contempla la activación del plan de continuidad del negocio cuando los incidentes tienen un impacto grave lo que evidencia integración del procedimiento con la gestión de continuidad y resiliencia institucional

La inclusión de indicadores de desempeño como el porcentaje de incidentes solucionados mensualmente refuerza el principio de mejora continua ya que permite evaluar la eficacia del procedimiento y compararlo contra metas establecidas este tipo de mediciones facilita que la alta dirección y la OTSI cuenten con información objetiva para tomar decisiones y asignar recursos de forma priorizada

El procedimiento fomenta la retroalimentación a través de la documentación de lecciones aprendidas lo que convierte cada incidente en una oportunidad de fortalecimiento del sistema y asegura que los errores o vulnerabilidades detectadas no se repitan consolidando un aprendizaje organizacional que es clave para el crecimiento en madurez de la gestión de la seguridad.

3. Manual de Gestión de Incidentes de Seguridad de la Información ST-MA-04 versión 01

El Manual, ST-MA-04 en su versión 01, constituye un documento sólido que fortalece el marco del SGSI del Ministerio de Educación Nacional porque se centra en proveer una guía estructurada para atender de manera ordenada los incidentes de seguridad y lo hace a través de un objetivo bien definido que contempla todas las fases críticas del ciclo de vida de un incidente desde la preparación hasta el seguimiento y las lecciones aprendidas lo cual asegura una gestión integral alineada con la norma ISO/IEC 27001:2022 y con las mejores prácticas internacionales.

En cuanto a la documentación del procedimiento se concluye lo siguiente:
El alcance resulta pertinente porque no limita la gestión a ciertos activos o plataformas específicas, sino que se extiende a todos los activos de información sin importar clasificación ni ubicación y además involucra a servidores contratistas y terceros que tengan acceso lo que fortalece el principio de universalidad y garantiza que ninguna brecha quede fuera del control institucional este enfoque amplía la cobertura del SGSI y refuerza la corresponsabilidad de todos los actores.

La política de gestión de incidentes incluida en el documento es un valor agregado ya que establece compromisos claros relacionados con la protección de activos la documentación de incidentes la adopción de medidas correctivas y la ejecución de acciones posteriores que

permitan mejoras continuas la obligación de analizar eventos verificar procedimientos clasificar incidentes y retener evidencias digitales aporta confianza en que el procedimiento no solo reacciona a los problemas sino que también impulsa el aprendizaje y la prevención.

La sección de definiciones constituye un aporte relevante porque homologa criterios y evita interpretaciones ambiguas al precisar la diferencia entre evento e incidente de seguridad y al clasificar los incidentes en categorías como acceso no autorizado código malicioso denegación de servicios mal uso de recursos tecnológicos y análisis de vulnerabilidades esta categorización facilita la detección temprana y la respuesta adecuada ya que los responsables pueden ubicar rápidamente el tipo de amenaza y aplicar las medidas correspondientes.

La inclusión de una matriz RACI que detalla roles responsabilidades y niveles de participación de cada actor institucional fortalece la coordinación porque asigna funciones específicas a la OTSI a la mesa técnica a control interno a la oficina jurídica a los servidores y contratistas y a otras áreas de apoyo esta claridad minimiza duplicidades mejora la comunicación y asegura que las decisiones y acciones cuenten con respaldo y trazabilidad dentro del marco organizacional.

El manual también se destaca por definir una metodología estructurada en cinco fases preparación detección contención erradicación y recuperación y seguimiento lo cual refleja un ciclo de gestión completo y coherente con los marcos de referencia como NIST SP 800-61 o ITIL Security Management cada fase incorpora actividades claras recursos herramientas tiempos de atención y matrices de actuación que permiten ordenar la respuesta y garantizar que los incidentes se atiendan en los plazos acordados.

En la fase de preparación se evidencian medidas concretas como la implementación de firewalls perimetrales antivirus antimalware controles de acceso y herramientas de análisis de vulnerabilidades que refuerzan la postura de defensa preventiva de la entidad lo cual contribuye a reducir la probabilidad de materialización de amenazas y aumenta la capacidad de resiliencia del entorno tecnológico institucional.

La fase de detección aporta valor al establecer tiempos máximos de atención según la criticidad del incidente con escalas desde muy grave hasta no importante lo que permite priorizar esfuerzos de respuesta de acuerdo con el impacto potencial además la integración de la detección con roles responsables asegura que el flujo de información sea oportuno y que las acciones se activen sin demoras.

Las fases de contención erradicación y recuperación son un punto fuerte porque no se limitan a detener el incidente, sino que buscan eliminar la causa raíz y restaurar los sistemas a su estado normal incluyendo pruebas de vulnerabilidad actualizaciones y mejoras de auditoría este enfoque contribuye a que los incidentes no se repitan y que la infraestructura tecnológica quede más fortalecida después de cada evento.

Para terminar, la fase de seguimiento refuerza la transparencia y la rendición de cuentas ya que establece informes periódicos a instancias de gestión comités técnicos y directivos además contempla indicadores específicos como el porcentaje de incidentes graves cerrados y el

porcentaje de incidentes normales atendidos que permiten medir objetivamente la eficacia de la gestión y facilitan la toma de decisiones basada en evidencia.

4. Formato de bitácoras de eventos ST-FT-21 – Versión 1

El formato ST-FT-21, Bitácora de eventos está diseñado como una herramienta de registro operativo para la gestión de incidentes y eventos de seguridad de la información dentro del SGSI y se presenta en un esquema tabular que facilita la trazabilidad de cada caso desde su detección hasta su resolución lo que lo convierte en un soporte fundamental para cumplir con los principios de documentación exigidos por la ISO/IEC 27001:2022.

En cuanto a la estructura del formato se concluye lo siguiente:

El documento inicia con un encabezado que identifica la bitácora de eventos e incorpora contadores de incidentes presentados respondidos resueltos y pendientes lo que aporta una visión ejecutiva rápida del estado de la seguridad en un periodo determinado y ofrece un valor agregado porque convierte al formato en un instrumento de monitoreo que trasciende el simple registro y facilita la toma de decisiones a nivel táctico y estratégico.

La estructura de los campos incluidos refleja una cobertura amplia y pertinente ya que contempla información como el analista responsable, el número de caso, la fecha y la severidad lo que asegura que cada evento tenga un responsable asignado y que pueda ser priorizado según su criticidad además se incluyen campos para servicio afectado asignatario dispositivo o URL descripción del evento y canal de notificación lo que fortalece la trazabilidad y permite reconstruir con claridad la cronología del incidente.

También prevé variables para estado actual, fecha de solución, área y persona que responde aplicación afectada solución y observaciones lo que garantiza no solo el seguimiento del ciclo de vida del incidente sino también la documentación de medidas correctivas aplicadas y la identificación de responsables de respuesta, ya que asegura facilita el seguimiento sobre la eficacia de la gestión de incidentes.

Un aspecto relevante es la inclusión de campos específicos como llamada telefónica que permiten registrar el medio de reporte o confirmación de incidentes lo cual enriquece la evidencia reforzando la eficacia del proceso de respuesta.

5. Roles y Responsabilidades en Seguridad de la Información ST-FT-15 – Versión 1.

El formato ST-FT-15, versión 01 corresponde a la definición de roles y responsabilidades en seguridad de la información, y se constituye en un instrumento de apoyo para el Sistema de Gestión de Seguridad de la Información porque permite alinear funciones, competencias y requisitos con la operación del SGSI, garantizando que cada actor institucional comprenda con claridad su papel en la protección de la información.

En cuanto a la estructura del formato se concluye lo siguiente:

El documento presenta un objetivo explícito, que es describir y formalizar los roles, funciones y competencias asociados a la seguridad de la información, lo cual asegura trazabilidad y orden en la gestión de talento humano, evitando ambigüedades sobre responsabilidades y facilita tanto la capacitación como la evaluación de desempeño en temas de seguridad.

La estructura del formato es un punto fuerte, ya que se organiza en columnas que incluyen formación o entrenamiento, experiencia, educación, habilidades, responsabilidades, rol y actividades, estableciendo así un marco completo de competencias. Esta distribución permite evaluar integralmente el perfil requerido, lo que resulta coherente con los requisitos de la norma ISO/IEC 27001:2022 en su cláusula 7.2 sobre competencia y concientización.

El valor añadido de este formato es que no solo define el rol y sus actividades, sino que también vincula estos elementos con requisitos de competencia, facilitando la planeación de capacitaciones, la asignación de responsabilidades y la selección de personal. Al mismo tiempo, constituye una evidencia documental clave para auditorías internas y externas, ya que demuestra que la entidad asegura la idoneidad de quienes intervienen en la gestión de seguridad.

VII. MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN

Durante las vigencias de agosto 2024 y junio 2025, la Oficina de Tecnología y Sistemas de Información documentó y formalizó las siguientes actividades en el marco del seguimiento institucional:

- Realizaron seguimiento al Plan de Acción Institucional, a través a los indicadores de gestión.
- Participaron en las sesiones del Comité Institucional de Gestión y Desempeño, efectuando seguimiento a los objetivos y metas institucionales.
- Verificaron los avances de los proyectos de transformación digital y de conectividad escolar, consolidando los resultados alcanzados en el periodo.
- Socializaron los informes de seguimiento con las dependencias involucradas, coordinando acciones de mejora para optimizar los procesos de gestión tecnológica e institucional
- Consolidaron reportes semanales de seguimiento de cambios, discriminando por ambiente (producción, certificación, pruebas), tipos de cambio (estándar, urgente) y aplicaciones más afectadas.

VIII. PARTICIPACIÓN CIUDADANA

Se constató que la Oficina de Tecnología y Sistemas de Información cumple con lo dispuesto en la Ley Estatutaria 1757 del 6 de julio de 2015 ("Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática"). Este cumplimiento se materializa, entre otros aspectos, en la gestión y mantenimiento técnico del micrositio "Participa" ubicado dentro de la página oficial del Ministerio de Educación Nacional. Dicha plataforma proporciona acceso a información acerca de los mecanismos, espacios y actividades que el Ministerio desarrolla para promover la participación ciudadana a lo largo del ciclo de gestión pública: diagnóstico, formulación, implementación, evaluación y seguimiento.

Adicionalmente, se encontró que el Ministerio ha establecido múltiples canales electrónicos de atención al público, cuya operación técnica depende íntegramente de esta Oficina. Entre ellos se incluyen:

- Correo electrónico, con la dirección dedicada para recibir PQRSDF: atencionalciudadano@mineducacion.gov.co.
- Chat en línea, disponible para consultas y orientación inmediata.

La gestión técnica y operativa de estos canales refuerza la transparencia y accesibilidad institucional, facilitando la interacción ciudadana y conectando directamente con los procesos de atención de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias. La Oficina de Tecnología garantiza así que dichos canales permanezcan activos, funcionales y actualizados, contribuyendo de manera efectiva al fortalecimiento de la participación democrática y la eficiencia en el acceso a la información pública.

IX. ESTADO DE LAS PETICIONES, QUEJAS, RECLAMOS, SUGERENCIAS Y DENUNCIAS

Se efectuó seguimiento a los informes generados por la Subdirección de Relacionamiento con la Ciudadanía, relacionados con la gestión de las Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD) por parte de la Oficina de la Oficina de Tecnología y Sistemas de Información:

MES / AÑO (PQRSD)	REPORTE	OBSERVACIÓN OCI
Agosto de 2024	• Total, comunicaciones: 237. • Cumplimiento de oportunidad: 92,83%. • Ranking: puesto 18. • Extemporáneos: 17 cerrados y 3 abiertos.	El área mantuvo un buen desempeño (92,83%), sin embargo, la presencia de 20 comunicaciones extemporáneas, de las cuales tres permanecieron abiertas, evidenció dificultades en el control de tiempos. Estos rezagos, aunque no comprometen gravemente los indicadores, representan un riesgo en caso de incrementarse.
Septiembre de 2024	• Total, comunicaciones: 202. • Cumplimiento de oportunidad: 96,53%. • Ranking: puesto 14.	Este mes presentó uno de los mejores desempeños del semestre, con 96,53% de oportunidad y sin rezagos abiertos. La oficina mostró control sobre su gestión, con mejoras frente a agosto. Este comportamiento muestra que, con seguimiento adecuado, los atrasos se reducen significativamente.
Octubre de 2024	Total, comunicaciones: 225. Cumplimiento de oportunidad: 89,78%. Ranking: puesto 28. Extemporáneos: varios cierres y con observaciones.	El desempeño descendió al 89,78% y la oficina cayó al puesto 28 en el ranking. Se evidenciaron cierres extemporáneos en algunos casos, lo que afecta la trazabilidad y expone a la entidad a riesgos frente a tutelas. Este retroceso marca la necesidad de reforzar el seguimiento en cierres correctos en el SGDEA.
Noviembre de 2024	• Total, comunicaciones: 254. • Cumplimiento de oportunidad: 93,31%. • Ranking: puesto 19. • Extemporáneos: 22 (16 cerrados, 6 abiertos).	La gestión mejoró respecto a octubre, alcanzando 93,31%. No obstante, seis rezagos abiertos al cierre del mes demuestran que aún existen cuellos de botella en la atención oportuna. Se observa que el aumento de volumen de comunicaciones impacta el control interno.
Diciembre de 2024	• Total, comunicaciones: 254. • Cumplimiento de oportunidad: 93,31%. • Ranking: puesto 19. • Extemporáneos: 22 (16 cerrados, 6 abiertos).	El mes cerró con una mejora significativa, alcanzando el 95,27% de oportunidad. No se registraron documentos abiertos de vigencias anteriores ni pendientes por recibir, lo cual refleja un cierre de año más ordenado. Aun así, es necesario mantener la disciplina en el SGDEA.

MES / AÑO (PQRSD)	REPORTE	OBSERVACIÓN OCI
Enero de 2025	• 287 comunicaciones. • Cumplimiento 89,90%. • Puesto 23 en ranking. • 29 extemporáneos • (17 abiertos, 12 cerrados).	La dependencia inició el año con un desempeño de oportunidad (89,90%), pero de los 29 documentos extemporáneos, 17 abiertos, evidencian falencias en el seguimiento interno. El volumen de rezagos contempló una tutela, que podría haber causado la materialización de un riesgo.
Febrero de 2025	• 286 comunicaciones. • Cumplimiento 75,52%. • Puesto 28 en ranking. • 70 extemporáneos • (16 abiertos, 54 cerrados).	El cumplimiento cayó a 75,52% y se observaron radicados con retrasos, principalmente en conceptos de memorando y comunicaciones internas. La carga de trabajo se concentró en un grupo reducido de funcionarios o contratistas para atender las solicitudes internas, lo que contribuyó a los atrasos.
Marzo de 2025	• 316 comunicaciones. • Cumplimiento 93,67%. • Puesto 18 en ranking. • 20 extemporáneos (6 abiertos, 14 cerrados).	La gestión mostró una recuperación con 93,67% de cumplimiento, aunque se mantuvo un rezago de 20 documentos extemporáneos. La existencia de radicados abiertos indica que, aunque mejoraron, aún persisten debilidades en la disciplina operativa y en la gestión de tiempos legales.
Abril de 2025	• 244 comunicaciones. • Cumplimiento 81,15%. • Puesto 26 en ranking institucional. • 198 comunicaciones atendidas a tiempo. • 46 extemporáneas.	Se observó un cumplimiento del 81,15%, que ubica a la dependencia en el puesto 26 del ranking. Aunque la mayoría de las comunicaciones fueron atendidas dentro del plazo (198), la existencia de 46 radicados extemporáneos refleja deficiencias en el control de vencimientos. Este resultado interrumpe la tendencia de mejora alcanzada en marzo, lo que indica que aún no se han consolidado mecanismos sostenibles de gestión documental.
Mayo de 2025	• 252 comunicaciones. • Cumplimiento 95,24%. • Puesto 16 en ranking. • 12 extemporáneos cerrados • Persisten retrasos	Aunque el indicador de oportunidad alcanzó el 95,24%, se evidenció un número considerable de radicados cerrados fuera de término, principalmente derechos de petición y conceptos especializados.

MES / AÑO (PQRSD)	REPORTE	OBSERVACIÓN OCI
Junio de 2025	• 153 comunicaciones. • Cumplimiento 97,39%. • Puesto 12 en ranking. • Extemporáneos cerrados con entre 6 y 16 días.	La OTSI alcanzó su mejor desempeño del semestre con 97,39% de cumplimiento. Sin embargo, se identificaron extemporáneos, incluyendo derechos de petición.

Fuente: SGDEA-Elaboración propia de la Oficina de Control Interno

El periodo comprendido entre agosto de 2024 y junio de 2025 muestra un comportamiento irregular en la gestión de las Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD):

MES / AÑO	RECIBIDAS	A TIEMPO	EXTEMP.	% OPORTUNIDAD
agosto-24	237	220	17	92,83%
septiembre-24	202	195	7	96,53%
octubre-24	225	202	23	89,78%
noviembre-24	254	237	17	93,31%
diciembre-24	275	262	13	95,27%
enero-25	287	258	29	89,90%
febrero-25	286	216	70	75,52%
marzo-25	316	296	20	93,67%
abril-25	244	198	46	81,15%
mayo-25	252	240	12	95,24%
junio-25	153	149	4	97,39%
TOTAL	2731	2473	258	90,96%

Fuente: Elaboración propia de la Oficina de Control Interno

Debido a que durante agosto y septiembre de 2024 se alcanzaron resultados destacados, con niveles de cumplimiento superiores al 92% y un máximo de 96,53% en septiembre. No obstante, en octubre el indicador descendió a 89,78%, reflejando dificultades en el control de los tiempos de respuesta.

En noviembre y diciembre de 2024 se observó una recuperación gradual, cerrando el año con un cumplimiento de 95,27% y sin rezagos abiertos, lo cual evidenció una capacidad de ajuste positivo. Sin embargo, en enero de 2025 se identificaron 29 comunicaciones extemporáneas, dentro de las cuales se encontró una tutela atendida fuera de término, lo que representa un posible riesgo. En febrero, la situación se agravó con un cumplimiento de apenas 75,52%, marcado por múltiples atrasos en derechos de petición y comunicaciones internas.

A partir de marzo de 2025 se evidenció una mejora progresiva, alcanzando 93,67% de cumplimiento, aunque en abril se presentó una nueva caída al 81,15%. En mayo y junio la oficina mostró su mejor desempeño, con resultados de 95,24% y 97,39% respectivamente, consolidando una recuperación sostenida y un ascenso en el ranking institucional.

La Oficina de Tecnología y Sistemas de Información demostró capacidad de recuperación y ajuste en su indicador, pero persisten rezagos derivados de la atención extemporánea de trámites sensibles, como tutelas, derechos de petición y comunicaciones internas. Para garantizar un desempeño sostenido y alcanzar el 100% de oportunidad, se requiere fortalecer los controles de seguimiento, optimizar la distribución de cargas de trabajo y reforzar el cumplimiento de plazos en todas las modalidades de comunicaciones.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES	RECOMENDACIONES
COMPONENTES DE RIESGOS Y EVALUACIÓN DE CONTROLES **Riesgos de Gestión:** Los riesgos de gestión tecnológica analizados se centran en tres escenarios principales: la indisponibilidad de los servicios TIC, la afectación por ataques informáticos y las fallas de infraestructura tecnológica. En todos los casos, la valoración inherente muestra una probabilidad baja a media, pero con impactos catastróficos que sitúan estos riesgos en zonas extremas o moderadas. Los controles implementados, tales como el monitoreo mensual de disponibilidad, la actualización trimestral del inventario de aplicaciones y la gestión de cambios, han permitido sostener niveles de disponibilidad superiores al 99,9 %. Igualmente, los informes técnicos evidencian atención oportuna de incidentes, aunque persisten debilidades por obsolescencia tecnológica, fallas en servidores críticos y bajo nivel de remediación de vulnerabilidades. En particular, la cobertura limitada en la gestión de vulnerabilidades y la ausencia de métricas de gestión (como MTTR y SLA) representan una amenaza latente para la continuidad y seguridad de los servicios. La gestión tecnológica evidencia madurez en la implementación de controles y cumplimiento de acuerdos de nivel de servicio. No obstante, el riesgo residual se	**Riesgos de Gestión:** Se recomienda establecer un plan integral de modernización tecnológica que contemple la actualización de sistemas y bases de datos obsoletos, así como la renovación planificada de servidores críticos. De igual forma, es fundamental implementar un programa de gestión de vulnerabilidades con métricas de desempeño claras (MTTR, SLA) que permitan medir y garantizar la efectividad de las acciones correctivas. Adicionalmente, fortalecer los planes de contingencia y de respuesta a incidentes asegurará la continuidad operativa frente a escenarios de alto impacto.

CONCLUSIONES	RECOMENDACIONES
mantiene elevado debido a la dependencia de infraestructura con vida útil superada y a la limitada capacidad de remediación de vulnerabilidades críticas. **Riesgo de Corrupción:** El riesgo de corrupción se refiere a la posibilidad de recibir o solicitar beneficios indebidos con el fin de manipular, filtrar o extraer información reservada de los sistemas institucionales. Aunque la probabilidad de materialización se clasificó como baja, el impacto es catastrófico, lo que sitúa este riesgo en una zona extrema. El análisis evidenció que, si bien se cuenta con informes de inteligencia de amenazas, despliegues de herramientas como Microsoft Defender y correlación de eventos en el SOC, persisten debilidades estructurales en la gestión de vulnerabilidades. La baja cobertura de remediación, problemas en la administración de certificados y protocolos criptográficos, así como la falta de trazabilidad en los cierres de vulnerabilidades, configuran un escenario en que podría convertirse en una amenaza real para la organización. El riesgo de corrupción no se ha materializado en el periodo auditado; sin embargo, la magnitud de las vulnerabilidades no remediadas y la deficiencia en la trazabilidad de los procesos mantienen un nivel de exposición elevado.	**Riesgo de Corrupción:** Se recomienda fortalecer la gestión de vulnerabilidades mediante la implementación de una trazabilidad completa, que permita documentar y verificar cada acción correctiva. Como prioridad, debe avanzarse en la remediación técnica de sistemas y aplicaciones críticas, complementada con el reforzamiento en la gestión de certificados y protocolos criptográficos para garantizar la seguridad de los entornos. De manera adicional, resulta necesario consolidar los controles de inteligencia de amenazas y asegurar el despliegue efectivo de herramientas de seguridad avanzada, de forma que estas medidas se integren en un marco robusto de prevención.
COMPONENTE DE PLANEACIÓN Y FINANCIERA **a) PRESUPUESTO** La ejecución presupuestal de la Oficina de Tecnología y Sistemas de Información durante el año 2024 se situó en un 59.70%. Este resultado según la OTSI explica, "*que Las Cuentas fueron radicadas y no se pagó por disponibilidad de PAC de diciembre.*" Constituyendo Cuentas Por Pagar y Reservas en un 40.09% equivalentes a $23.714 millones. La ejecución presupuestal de la OTSI al final del primer semestre de 2025 se sitúa en un 21.57%, significativamente por debajo del 50% esperado por	Fortalecer para la vigencia 2025 el seguimiento y la gestión de los contratos. asociados a los rubros de Adquisición de BYS – Servicio de Asistencia Técnica - 2. SEGURIDAD HUMANA Y JUSTICIA SOCIAL / F. GESTIÓN TERRITORIAL EDUCATIVA Y COMUNITARIA, SERVICIO DE IMPLEMENTACIÓN SISTEMAS DE GESTIÓN - FORTALECIMIENTO DE LA GESTIÓN INSTITUCIONAL Y BUEN GOBIERNO DEL MINISTERIO DE EDUCACIÓN NACIONAL entré otros. Se debe identificar y resolver cualquier obstáculo que esté impidiendo el avance en la ejecución de estos recursos, prestando

CONCLUSIONES	RECOMENDACIONES
principio de anualidad. Esta baja ejecución incluye rubros de contratos con un (0%).	especial atención a los contratos con ejecución (0) %.
b) INDICADORES La evaluación de los indicadores evidencia un desempeño globalmente favorable y alineado con los objetivos estratégicos: En materia de transformación digital, se alcanzaron las metas establecidas, consolidando iniciativas que reflejan capacidad técnica, articulación institucional y sostenibilidad en el tiempo. El indicador de conectividad escolar muestra avances significativos, aunque persisten limitaciones en algunas secretarías que no presentan proyectos o no atienden oportunamente las observaciones técnicas, lo que afecta la cobertura total y puede comprometer el cumplimiento de la meta anual. Por su parte, el monitoreo del rendimiento de aplicaciones confirma altos niveles de estabilidad y disponibilidad en los sistemas priorizados, aunque su alcance reducido limita una visión integral del desempeño de todas las aplicaciones críticas de la entidad.	Se recomienda continuar con la estrategia integral de gestión tecnológica, centrada en tres ejes: asegurar la continuidad de las iniciativas de transformación digital, fortalecer el acompañamiento y la supervisión a las secretarías de educación en materia de conectividad escolar, y ampliar progresivamente el monitoreo de aplicaciones críticas. Esta estrategia debe orientarse a mejorar la cobertura, garantizar la sostenibilidad de los avances y reforzar la capacidad preventiva de la organización, en coherencia con los principios de mejora continua.
COMPONENTE DE CONTRATACIÓN Del análisis efectuado a los contratos revisados en las vigencias 2024 y 2025 se identificó que en algunos casos los informes presentaron un avance estático durante varios meses, particularmente en el contrato de apoyo en ingeniería de software, que permaneció con un reporte del 25% en los tres últimos cortes del año, reflejando un registro de ejecución limitado y poco representativo de la evolución real de las actividades. Igualmente, se evidenciaron inconsistencias en la denominación de los periodos de seguimiento, como el caso de un informe correspondiente a agosto que fue consignado como si perteneciera a julio, lo cual pone de manifiesto debilidades en la disciplina de reporte y en el seguimiento contractual.	Se recomienda fortalecer el proceso de supervisión contractual mediante la implementación de controles que eviten la presentación de informes con avances estáticos o inconsistencias en la denominación de periodos, asegurando que los reportes reflejen de manera real y verificable la ejecución de las actividades. También, es necesario garantizar conforme al manual de supervisión, CN-MA-02 en su versión 2, que el contratista "cumpla las directrices implementadas en el SGD, para el manejo integral de la información y que atienda con la oportunidad debida los

CONCLUSIONES	RECOMENDACIONES
Como buena práctica, el Ministerio tiene establecido el lineamiento de cargar los pantallazos del SGDEA en los informes de los contratos de OPS con el fin de garantizar la trazabilidad documental y la integridad en el manejo de la información; no obstante, se encontró que este procedimiento no se cumplió de manera uniforme, pues en varios contratos los soportes no fueron anexados en la plataforma SECOP II, afectando la completitud del ciclo documental de la entidad. Pese a estas debilidades, la revisión de los perfiles técnicos permitió concluir que se cumplió con la experiencia exigida en los estudios previos, lo que garantiza que los profesionales vinculados contaran con la idoneidad necesaria para el desarrollo de las actividades contratadas y que la ejecución contractual se respaldara en capacidades técnicas adecuadas para atender los requerimientos del Proceso de Gestión de Servicios TIC.	radicados que le sean asignados en el marco de la ejecución del objeto pactado, de modo que el respectivo aplicativo de correspondencia se mantenga actualizado y al día". Por lo anterior, se sugiere dejar de acuerdo con los lineamientos de la oficina de contratación, pantallazos del SGDEA en los informes de actividades, mostrándose al día en las respuestas oportunas como allí se indiquen, con relación a cada uno de los distintos requerimientos efectuados tanto internamente como externo.
COMPONENTE TECNOLÓGICO **Seguridad física y continuidad operativa:** Se constató que el Ministerio de Educación dispone de un sistema de climatización especializado mediante aires acondicionados de precisión, lo cual permite mantener de forma constante la temperatura y humedad en los rangos adecuados para equipos de misión crítica, reduciendo significativamente los riesgos de sobrecalentamiento o condensación. Adicionalmente, se ejecutan mantenimientos preventivos semestrales a racks, cableado estructurado y sistemas de energía, incluyendo la renovación de baterías de UPS con gestión ambiental certificada para su disposición final, lo que evidencia disciplina operativa y cumplimiento normativo. Estos controles aseguran la disponibilidad continua de la infraestructura y fortalecen la resiliencia frente a interrupciones.	**Seguridad física y continuidad operativa:** Seguir consolidando el esquema sólido de seguridad física y continuidad operativa, apoyado en sistemas de climatización de precisión, mantenimientos preventivos regulares y una gestión ambiental responsable de los equipos de respaldo. **Gestión de cambios y configuraciones:** Continuar con la gestión de cambios y configuraciones refleja un proceso maduro y confiable, sustentado en la trazabilidad documental y la participación de un comité

CONCLUSIONES	RECOMENDACIONES
Gestión de cambios y configuraciones: El control de cambios se gestiona a través de solicitudes formales (RFC) que son evaluadas y aprobadas por un comité especializado, considerando el análisis de riesgos y la programación en ventanas de mantenimiento. Este procedimiento aporta trazabilidad y reduce la probabilidad de modificaciones no autorizadas en la infraestructura crítica. Aunque los servidores no son administrados directamente por el equipo de infraestructura, se evidenció que los cambios relevantes en bases de datos y servicios de red siguen este esquema de autorización formal, lo cual demuestra un control robusto y alineado con la norma. **Respaldo y recuperación de información:** El sistema de respaldo implementado cuenta con diferentes frecuencias de ejecución (diaria, semanal, mensual y anual), con períodos de retención definidos que aseguran la disponibilidad histórica de la información. El esquema redundante, soportado en datacenters espejo ubicados en Bogotá y Tocancipá, fortalece la continuidad del servicio frente a fallas o contingencias. Además, la entidad dispone de un plan de pruebas de restauración en ejecución, con informes ya generados y validados, lo que garantiza la integridad de los respaldos y demuestra la efectividad de este control. **Transición de la 27001:2013 a la 27001:2022:** El Ministerio de Educación Nacional ha demostrado avances significativos del 80% en la transición de la norma ISO/IEC 27001:2013 hacia la versión 2022, evidenciados en la actualización de su contexto organizacional, la identificación de partes interesadas, el fortalecimiento de la gestión de riesgos y la incorporación progresiva de nuevos controles y políticas. Sin embargo, el SGSI aún presenta un grado de implementación parcial, con brechas en la formalización documental, la consolidación de la nueva política de seguridad de la información, la integración transversal de los requisitos de privacidad y ciberseguridad, así como en la consolidación de planes de tratamiento de riesgos.	especializado que vela por la seguridad y disponibilidad de los servicios **Respaldo y recuperación de información:** Seguir el esquema de respaldos implementado, con redundancia geográfica y pruebas de restauración validadas, demuestra un alto nivel de compromiso con la continuidad del servicio y la protección de la información. Acelerar la transición hacia la norma ISO/IEC 27001:2022 mediante la formalización y consolidación documental del SGSI dentro del Sistema Integrado de Gestión (SIG), asegurando la aprobación y socialización de la nueva política de seguridad de la información, la integración plena de los requisitos de privacidad y ciberseguridad, y la actualización de la Declaración de Aplicabilidad con los nuevos controles del Anexo A. De igual forma, se recomienda implementar un plan institucional de sensibilización y formación continua en seguridad de la

CONCLUSIONES	RECOMENDACIONES
Se reconoce el compromiso institucional y el respaldo de la alta dirección para avanzar en esta transición, pero es necesario acelerar la formalización de documentos, la consolidación del repositorio del SGSI en el SIG, la asignación de recursos adicionales y la adopción plena de los nuevos controles del Anexo A, de manera que se logre un cumplimiento integral de los requisitos de la ISO/IEC 27001:2022 y se fortalezca la resiliencia organizacional frente a amenazas emergentes y entornos digitales cambiantes	información, dirigido a todos los niveles organizacionales, que consolide la cultura de seguridad y facilite la apropiación de los nuevos lineamientos. Con estas acciones, la Entidad podrá cerrar las brechas identificadas, cumplir oportunamente con los requisitos de la versión 2022 y robustecer su resiliencia frente a amenazas emergentes y cambios tecnológicos
MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN Periódicamente se realizan reuniones de evaluación y autoevaluación, orientadas a identificar acciones de seguimiento y mejoramiento respecto de las debilidades y oportunidades detectadas. Igualmente, se evidenció que el análisis, la documentación y la conservación de las necesidades priorizadas de los usuarios se gestionan a través del sistema de gestión documental, complementado con la aplicación de encuestas basadas en datos abiertos**.**	Continuar con las buenas prácticas de realizar reuniones periódicas de evaluación y autoevaluación, fortaleciendo su alcance con mecanismos de seguimiento que permitan evidenciar los avances logrados frente a las acciones definidas.

Como resultado de la auditoría, se evidenció que la gestión adelantada por el proceso se desarrolla de manera adecuada y en concordancia con el marco regulatorio vigente. Se constató la aplicación de procedimientos y formatos que favorecen el cumplimiento de la gestión, así como la existencia de procedimientos documentados que contemplan y cumplen los puntos de control establecidos.

La auditoría se ejecutó conforme a lo establecido en el Plan de Auditoría, cumpliendo con el objetivo y el alcance definidos. Este resultado fue posible gracias a la disposición y colaboración de los profesionales que atendieron oportunamente los requerimientos del equipo auditor.

INFORME DETALLADO			
Resultado		**Descripción**	**Recomendación**
HZ	**OM**		
	X	**COMPONENTES DE RIESGOS Y EVALUACIÓN DE CONTROLES** Persisten aplicaciones, sistemas operativos y bases de datos desactualizados (PostgreSQL, Red Hat, Oracle, Windows), sin plena compatibilidad con IPv6. Además, algunos servidores críticos (hiperconvergentes y web hosting) superaron su vida útil y presentan fallas físicas en discos, reinicios inesperados de máquinas virtuales y sobrecargas recurrentes de CPU. Estas condiciones incrementan la probabilidad de indisponibilidad de servicios esenciales, afectando la continuidad operativa y aumentando el riesgo de pérdida de integridad y confidencialidad de la información crítica de la Entidad.	Realizar un análisis de factibilidad técnica y de compatibilidad que permita evaluar los riesgos, costos y beneficios de la modernización de sistemas operativos, motores de bases de datos y lenguajes de programación, asegurando su alineación con los estándares actuales y la integración con IPv6, con el fin de garantizar la estabilidad y continuidad de las aplicaciones institucionales. De igual forma, efectuar un estudio de capacidad y resiliencia de la infraestructura crítica (servidores hiperconvergentes y de web hosting) que contemple escenarios de carga, disponibilidad y contingencia, para definir un plan progresivo de modernización encaminado a fortalecer el procesamiento y almacenamiento de los servidores críticos que fortalezca la continuidad operativa y reduzca la exposición a fallas técnicas. El resultado deberá ser presentado a la alta dirección y/o áreas funcionales, para su revisión dentro del plan de modernización tecnológica de la Entidad.
X		**COMPONENTES DE RIESGOS Y EVALUACIÓN DE CONTROLES** El nivel de remediación de vulnerabilidades críticas es bajo, alcanzando solo un 5 % de cierre frente a las 4.852 detectadas en 396 activos críticos. Esta situación incrementa la superficie de ataque y expone a la organización a riesgos de indisponibilidad, pérdida de	Implementar una acción correctiva que priorice la atención de vulnerabilidades críticas usando métricas como CVSS e impacto al negocio, con tiempos máximos de remediación diferenciados según la severidad.

INFORME DETALLADO			
Resultado		**Descripción**	**Recomendación**
HZ	**OM**		
		confidencialidad e integridad de la información.	
	X	**PRESUPUESTO** La ejecución presupuestal de la Oficina de Tecnología y Sistemas de Información durante el año 2024 se situó en un 59.70%. Este resultado según la OTSI explica, "que Las Cuentas fueron radicadas y no se pagó por disponibilidad de PAC de diciembre." Constituyendo Cuentas Por Pagar y Reservas en un 40.09% equivalentes a $23.714 millones. La ejecución presupuestal de la OTSI al final del primer semestre de 2025 se sitúa en un 21.57%, significativamente por debajo del 50% esperado por principio de anualidad. Esta baja ejecución incluye rubros de contratos con un (0%).	Generar acciones en aras de garantizar una adecuada planeación presupuestal y programación de pagos que permitan la ejecución oportuna de los recursos asignados a la OTSI, evitando la acumulación de cuentas por pagar. Adicionalmente, se sugiere la continua monitorización del avance presupuestal a nivel de obligaciones mediante alertas tempranas, con el fin de lograr una ejecución más eficiente y alineada con el principio de anualidad y los objetivos estratégicos de la oficina.
	X	**ESTADO DE LAS PETICIONES, QUEJAS, RECLAMOS, SUGERENCIAS Y DENUNCIAS** De acuerdo con los informes de la Subdirección de Relacionamiento con la Ciudadanía, la gestión de las PQRSD en el periodo agosto 2024 – junio 2025 presentó un promedio de cumplimiento del 90,96 % en la oportunidad de respuesta. No obstante, se identificaron caídas significativas en meses como febrero (75,52 %) y abril de 2025 (81,15 %), lo que evidencia rezagos en trámites sensibles, incluyendo tutelas y derechos de petición externos.	Optimizar el proceso de atención de PQRSD mediante la implementación de una acción de mejora integral que permita descongestionar los trámites acumulados, y garantizar la respuesta en los tiempos establecidos por la Entidad. Para ello, se sugiere incorporar alertas manuales o automáticas para que generen comunicados informativos de manera temprana sobre vencimientos de los radicados.

NOTA: El cuadro anterior se diligencia solo para auditorías de Gestión.

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
X			4 -CONTEXTO DE LA ORGANIZACIÓN	El Ministerio de Educación tiene definido su contexto a través del Manual de Políticas de Seguridad Digital y de procedimientos como la gestión de incidentes y de cambios, estableciendo lineamientos orientados a la protección de la confidencialidad, integridad y disponibilidad de la información con un enfoque en los activos tecnológicos y en los procesos internos de tecnología, orientando sus acciones a la continuidad operativa, la identificación de riesgos técnicos y el cumplimiento de normativas básicas de seguridad digital. En la transición a la versión ISO/IEC 27001:2022 se consolida el análisis del contexto al incluir factores internos y externos que afectan al SGSI mediante el documento "Contexto Organizacional", donde se identifican las partes interesadas, sus requisitos y la relación con los objetivos estratégicos del Ministerio. Este ejercicio permite integrar la seguridad y privacidad de la información con lineamientos del MINTIC y el MSPI, avanzando hacia un modelo más integral. No obstante, la formalización y control documental aún están en proceso, lo que refleja una madurez progresiva en la adopción de la norma
X			5 – LIDERAZGO	El liderazgo de la organización se refleja en el compromiso de la alta dirección mediante la definición de responsabilidades formales, la asignación de recursos y la emisión de lineamientos que sustentan el funcionamiento del SGSI, lo cual queda evidenciado en los documentos de gestión de incidentes a través del Manual ST-MA-04 V1 y el procedimiento ST-PR-18 V2, donde se establecen roles y responsabilidades a través de matrices RACI. Ahora en la transición a la versión ISO/IEC 27001:2022 se fortalece el liderazgo institucional al proyectar una nueva política de seguridad de la información que incorpora objetivos específicos,

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
				medibles y alineados con la estrategia institucional. Aunque actualmente se dispone de un manual de seguridad digital en uso, se reconoce la necesidad de evolucionar hacia un documento que abarque integralmente la ciberseguridad y la privacidad. El compromiso de la alta dirección se evidencia en la asignación de roles, recursos y actividades de sensibilización, destacando simulaciones prácticas como pruebas de phishing que fortalecen la cultura organizacional
X			6- PLANIFICACIÓN	El Ministerio de Educación Nacional desarrolla la planificación del SGSI a partir del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, donde se definen objetivos, marco normativo y metodología de gestión de riesgos, con criterios de probabilidad e impacto y opciones de tratamiento como aceptar, reducir, evitar o transferir. Además, contempla medidas como escaneos de vulnerabilidades, aplicación de planes de mitigación priorizados por criticidad y seguimiento de riesgos a través del SIG y el MIPG, asegurando trazabilidad y actualización continua. Esta también se integra en los procedimientos operativos: el de Gestión de Cambios (ST-PR-12) exige evaluar riesgos y prever planes de reversa; el de Gestión de Incidentes (ST-PR-18) retroalimenta la planificación mediante lecciones aprendidas; y el de Gestión de Seguridad de la Información (ST-PR-08) incorpora la clasificación de activos y definición de controles. Además, la Guía ST-GU-16 establece requisitos de seguridad para proveedores que deben incluirse en la planeación de servicios tercerizados. En la transición a la versión ISO/IEC 27001:2022 se robustecen los procesos de planificación al actualizar la metodología de gestión de riesgos con criterios más amplios que incluyen variables financieras, reputacionales y de impacto en la privacidad. La

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
				actualización de la Declaración de Aplicabilidad y la consolidación de planes de tratamiento de riesgos reflejan la intención de alinear el SGSI con los nuevos controles del Anexo A. Aunque aún se requieren mayores niveles de formalización y recursos, se evidencia un avance hacia un modelo preventivo y estratégico
X			7- SOPORTE	El Ministerio garantiza el soporte del SGSI mediante la definición de roles y responsabilidades, programas de formación y sensibilización, y el aseguramiento de recursos tecnológicos y documentales. En el ámbito de concienciación, se cuenta con la estrategia *PM-PR-07* para promover la cultura de seguridad de la información en la entidad, dirigida a funcionarios y contratistas. Para la gestión de proveedores, se dispone de la *Guía ST-GU-16*, que establece los requisitos mínimos de seguridad que deben cumplir los terceros, incluyendo acuerdos de confidencialidad y controles de continuidad. A nivel documental, los manuales y procedimientos del SGSI se encuentran registrados como copias controladas en el SIG, lo que asegura el control de versiones y su disponibilidad para los usuarios autorizados. De este modo, la entidad asegura que las competencias, recursos, comunicaciones y controles documentales se articulen al servicio de la gestión de seguridad de la información. En la transición a la versión ISO/IEC 27001:2022 se refuerza el soporte al SGSI mediante la integración de recursos tecnológicos y humanos suficientes, con presupuesto y con perfiles técnicos definidos para la operación del sistema. La gestión documental, la comunicación institucional y las actividades de concienciación demuestran un compromiso sostenido. Además, se fortalece la relación con proveedores y terceros a través de cláusulas contractuales y

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
				lineamientos de seguridad, lo que amplía la cobertura del soporte del sistema
X			8- OPERACIÓN	La operación del SGSI se materializa a través de procedimientos específicos que garantizan la ejecución controlada de las actividades. Entre ellos destacan: el procedimiento *ST-PR-08 Gestión de Seguridad de la Información*, que regula la identificación, clasificación y protección de activos; el *ST-PR-18 Gestión de Incidentes de Seguridad de la Información*, que establece las fases de detección, reporte, análisis, contención, erradicación, recuperación y lecciones aprendidas; y el *ST-PR-12 Gestión de Cambios*, que regula la evaluación técnica de solicitudes, la justificación, las aprobaciones, la realización de pruebas y el plan de reversa en caso de fallas. Todos estos procedimientos están integrados al SIG y permiten garantizar trazabilidad, control y respuesta sistemática ante riesgos operativos y tecnológicos, alineando la operación del SGSI con los procesos institucionales. En la transición a la versión ISO/IEC 27001:2022 se optimiza la operación del SGSI mediante la incorporación de tecnologías emergentes, controles avanzados y la sistematización de procesos como gestión de incidentes y cambios. Se destacan prácticas como el fortalecimiento de la seguridad perimetral, la autenticación multifactor y el monitoreo continuo, que evidencian la capacidad de adaptación frente a amenazas emergentes. La operación deja de ser reactiva para convertirse en un proceso dinámico con trazabilidad, control y retroalimentación permanente.
			9- EVALUACIÓN	La entidad ha definido actividades de seguimiento, medición y revisión del SGSI. El *Plan de Tratamiento de Riesgos* contempla revisiones periódicas, seguimiento a los controles implementados y planes

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
X				de mejoramiento continuo que se cargan en el SIG para su trazabilidad. Asimismo, se realizan actividades de monitoreo como escaneos de vulnerabilidades y análisis de impacto, cuyos resultados son socializados con líderes de proceso. Los avances y hallazgos se presentan en el Comité Institucional de Gestión y Desempeño, donde se toman decisiones sobre acciones correctivas y asignación de recursos. De esta manera, el Ministerio mantiene un esquema de evaluación continua del desempeño del SGSI, articulado con sus mecanismos de gestión institucional. Como parte de esta transición, se está trabajando en la documentación del Plan de Recuperación ante Desastres (DRP) y en el análisis de impacto en el negocio (BIA), contemplando una fase 2 de pruebas para validar la efectividad de las medidas definidas. Paralelamente, se realiza seguimiento a planes de mejoramiento y a la gestión de riesgos, incorporando ajustes derivados de amenazas emergentes y cambios normativos.

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
X			10 - MEJORA	El compromiso con la mejora continua se evidencia en la implementación del *Planes de mejoramiento* asociado al SGSI, el cual recoge hallazgos en seguimientos, auditorias, autoevaluación, y los traduce en acciones correctivas y preventivas. Estas acciones se priorizan con base en la criticidad de los riesgos identificados y se cargan en el SIG para su seguimiento y control. Con este mecanismo, el Ministerio asegura que el SGSI evolucione continuamente y se adapte a los nuevos escenarios tecnológicos y regulatorios, garantizando la resiliencia institucional en materia de seguridad de la información. Para la transición a la versión ISO/IEC 27001:2022 se potencia la mejora continua con planes de acción priorizados según criticidad y articulados con el SIG. La implementación de revisiones periódicas, la actualización documental y la inclusión de pruebas de recuperación ante desastres demuestran una evolución hacia un SGSI resiliente y en constante aprendizaje. La mejora deja de ser reactiva para consolidarse como un proceso planificado, trazable y sostenible

NOTA: El cuadro anterior se diligencia solo para auditorías de Gestión.

AUDITORÍA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
N.A.	N.A.	N.A.	N.A.	N.A.

LÍDER DEL EQUIPO AUDITOR: WILLIAM MONROY RINCON

JEFE OFICINA DE CONTROL INTERNO: MARCELA LATORRE CANO