La educación es de todos Mineducación	**INFORME DE AUDITORÍAS**	**Código: EAD-FT-07** **Versión: 05** Rige a partir de su publicación en el SIG

INFORME DE AUDITORÍA											
Proceso:				**Gestión de Servicios TIC**							
Numero de Auditoria:				2021-G-03							
Reunión de Apertura						**Reunión de Cierre**					
Día	12	**Mes**	07	**Año**	2021	**Día**	09	**Mes**	11	**Año**	2021

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):
Roger Quirama Garcia/ Jefe Oficina de Tecnología y Sistemas de Información

EQUIPO AUDITOR *(Registrar datos del líder de auditoria y equipo auditor de apoyo – Aplica para Auditorias de Modelos referenciales y Auditorias de Gestión).*
AUDITOR LÍDER:

- Mónica Alexandra González Moreno

AUDITOR DE APOYO:

- Luz Yanira Salamanca

OBJETIVO DE AUDITORÍA:

Verificar la eficacia de los controles establecidos para gestionar las necesidades y la calidad de los productos tecnológicos, con el propósito de retroalimentar en cuanto a oportunidades de mejora que contribuyan al cumplimiento de los objetivos estratégicos definidos por la Entidad.

ALCANCE DE AUDITORÍA:

El alcance de la auditoría al proceso de "Gestión de Servicios TIC", comprende la revisión de los siguientes aspectos:

Procedimiento Gestión de Configuración Código SIG. ST-PR-10 V.04
Procedimiento Gestión de Capacidad Código SIG: ST-PR-03 V.01
Plan de Capacidad Código SIG: ST-PL-02 V.03
Plan de Acción Institucional
Mecanismos de Autoevaluación y Autocontrol
Matriz de Riesgos del Proceso de Gestión y de Corrupción
Activos de Información y Seguridad Digital

El periodo definido como objeto de revisión es el comprendido el 1º de julio de 2020 a 30 de junio de 2021

CRITERIOS DE AUDITORÍA:

- Procedimiento Gestión de Configuración Código SIG. ST-PR-10 V.04
- Flujograma Procedimiento Gestión de la Configuración Código SIG: ST-AN-06 V. 03
- Procedimiento - Gestión de Capacidad Código SIG: ST-PR-03 V.01
- Plan de Capacidad Código SIG: ST-PL-02 V.03
- Flujograma Procedimiento Gestión de Capacidad Código SIG: ST-AN-03 V.01
- Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas DAFP -V.05 diciembre 2020
- Guía de la Administración del Riesgo del Ministerio de Educación Nacional Código SIG: PM-GU-01 V.04

- Guía de gestión de riesgos “Seguridad de la Información” guía 7 MINTIC
- Plan de Acción Institucional-Guía de Seguimiento y Evaluación del Plan de Acción Institucional Código SIG: PL-GU-03, V.3
- Matriz de Riesgos de Seguridad Digital y Activos de Información
- Documento CONPES-CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA 3854 de 2016 Política Nacional de Seguridad Digital
- Guía de implementación de la política gobierno digital
- Ley de transparencia 1712 del 6 de marzo de 2014: "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”

Mejores Prácticas de Tecnología:

- ITIL versión 4 - Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información). Marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad.
- COBIT Version 5 (Control Objectives for Information and related Technology). Marco aceptado internacionalmente como buenas prácticas para el control de la información, TI y los riesgos que conllevan.

RESUMEN GENERAL

FORTALEZAS

Se evidenció la sincronización de las herramientas CA (mesa de ayuda) para el monitoreo de los elementos técnicos y tecnológicos que apoyan la gestión de los procesos del MEN.

Implementación y mejoras en cuanto a escritorios virtuales, Colombia Aprende, página web, prestamos de equipos, doble factor de autenticación, Microsoft Teams, VPN, lo cual permite una mejor prestación del servicio tanto a usuarios internos como a externos.

RIESGOS Y EVALUACIÓN DE CONTROLES*:*

Se realizó validación de los Riesgos de Gestión y de Corrupción del proceso de “Gestión de Servicios TIC” registrados en el Sistema Integrado de Gestión (SIG), evidenciando las siguientes situaciones:

Riesgos de Gestión

RIESGO Y CONTROLES	MONITOREO AL CONTROL	OBSERVACIONES DE LA OFICINA DE CONTROL INTERNO
RIESGO DE GESTION Afectación en la Integridad, confidencialidad y disponibilidad de los servicios Tecnológicos del MEN **CAUSAS** ✓ Pérdida de dispositivos móviles (celulares, tablets, portátiles, etc) con información contenida dentro de estos. ✓ Falta de Verificación de vulnerabilidades de los servicios TICs (Infraestructura, aplicaciones, bases de datos.) ✓ Incumplimiento de las políticas de seguridad y privacidad de la información ✓ Comprometer la información por un factor humano (Error en el uso de los sistemas de	**Actividades realizadas durante el periodo:** -Seguimiento a los servicios esenciales TI del MEN, del cual se genera el informe de seguimiento de gestión técnica infraestructura TI. -Se presenta el informe del servicio esencial de hyperconvergencia de	**Primera Línea de Defensa:** La Oficina de Tecnologia y Sistemas de Información realizó los seguimientos e informes con el fin de analizar la información sobre los niveles de calidad, validar la prestación y disponibilidad de los servicios de TI para evitar la materialización del riesgo “Afectación en la Integridad, confidencialidad y disponibilidad de los servicios Tecnológicos del MEN”. **Segunda Línea de Defensa:** La Subdirección de Desarrollo Organizacional realizó seguimiento sobre el

información, equipos de cómputo y de la información, Abuso de los roles y perfiles asignados, Suplantación de identidad, de roles y perfiles asignados, Negación de acciones, Incumplimiento en la disponibilidad del personal, etc.) ✓ Comprometer la información (Interceptación de la información, Espionaje remoto, Hurto de medios o documentos, Hurto de equipos de cómputo, Recuperación de medios reciclados o desechados, Divulgación no autorizada, Datos provenientes de fuentes no confiables, Manipulación con software Manipulación con hardware, etc.,.) ✓ Implementación de soluciones de seguridad perimetral y de antimalware ✓ Se cuenta implementados controles para el aseguramiento de los activos de información dentro de dispositivos móviles ✓ Incumplimiento de las políticas de seguridad y privacidad de la información ✓ Ataques Informáticos (Virus informáticos o código malicioso, Denegación de Servicios (DoS), Phishing, inyección de código, ataques de fuerza bruta, SPAM, etc.) ✓ Acciones no autorizadas (Uso no autorizado de los equipos de cómputo o comunicaciones. Copia fraudulenta del software o sistemas de información, Uso de software no autorizado por el MEN, Corrupción de los datos, Procesamiento ilegal de datos, etc.) ✓ Conocer e implementar nuevas tecnologías para el aseguramiento de los activos de información dentro de dispositivos móviles ✓ Contar con las soluciones tecnológicas para el escaneo de vulnerabilidades ✓ Conocer las nuevas tecnologías para la seguridad de los activos de información. **CONTROLES** ✓ Realizar seguimiento y evaluación mensual de la disponibilidad de los servicios esenciales TIC. ✓ Realizar seguimiento mensual a los contratos de servicios TIC. - Informe de disponibilidad, confiabilidad e integridad de los servicios contratados para el collocation de la infraestructura en el Datacenter externo y dispositivos de seguridad perimetral. - Informe de disponibilidad, confiabilidad e integridad de los servicios contratados de conectividad (internet, comunicaciones entre Datacenters, secretarías de educación, etc.) -Informe de disponibilidad, confiabilidad e integridad de los servicios de operación global de servicios Tics.	disponibilidad y uso por infraestructura, uso, soluciones, aplicaciones, sistemas de información del MEN. - Se presenta el informe del frente de seguridad el cual detalla los incidentes presentados - Se presenta el informe del plan de pentest realizado. - Se realizó el escaneo sobre aplicaciones y la infraestructura tecnológica del Ministerio, informe de vulnerabilidades.	adecuado diseño de los controles para la mitigación del riesgo identificado. Igualmente, se observó el seguimiento al reporte de evidencias reportadas en el Sistema Integrado de Gestión-SIG **Tercera Línea de Defensa:** La Oficina de Control Interno observó que el proceso monitorea el riesgo identificado, sin embargo, los controles establecidos para las causas identificadas no son suficientes frente a las mismas, situación que se evidencia en los productos entregados al equipo auditor. Se recomienda revisar y ajustar la matriz de riesgos del proceso de Gestión de Servicios TIC, teniendo en cuenta los cambios efectuados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5-diciembre 2020 del DAFP, en los siguientes aspectos: -Articular la institucionalidad de MIPG "Política Gobierno Digital" con la gestión del riesgo. -Ajustar la redacción del riesgo, causas y controles -Tener en cuenta la clasificación del riesgo en el momento de identificarlo. -Revisar los controles establecidos teniendo en cuenta los parámetros establecidos en la guía -Ajustar la redacción y diseño de las causas identificadas. -Ajustar la redacción, diseño y evaluación de los controles según la calificación. -Armonizar el tratamiento de los riesgos para cumplir con los objetivos estratégicos y de proceso de la entidad.

✓ Realizar seguimiento y evaluación de los incidentes de seguridad de la información relacionados con servicios TIC reportados por el equipo de seguridad del operador de servicios TIC. Este incluye un informe sobre la identificación del uso no autorizado de los equipos de cómputo o comunicaciones. ✓ Realizar seguimiento y evaluación trimestral de pruebas de penetración (pentesting) bajo responsabilidad del equipo de seguridad del operador de servicios TIC. ✓ Realizar seguimiento y evaluación trimestral de escaneo de vulnerabilidades a la infraestructura y sistemas de información del MEN. **EVALUACIÓN DEL RIESGO RESIDUAL** **Riesgo Residual**: Zona de Riesgo Alta **Acción de manejo:** Reducir el riesgo **PLAN DE ACCIÓN O DE MANEJO** Sensibilización semestral de las políticas de seguridad de la información por parte de los servidores y contratistas del MEN. Fecha de Inicio 1/01/2021 Fecha de Finalización: 31/12/2021 **Meta:** 1 **Porcentaje:** 100%		

Fuente: Matriz de riesgos SIG-Proceso "Gestión de Servicios TIC".

Riesgos de Corrupción

RIESGO Y CONTROLES	MONITOREO AL CONTROL	OBSERVACIONES DE LA OFICINA DE CONTROL INTERNO
RIESGO DE CORRUPCION 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 **CAUSAS:** ✓ Pérdida de dispositivos móviles (celulares, tablets, portátiles, etc) con información contenida dentro de estos. ✓ Falta de Verificación de vulnerabilidades de los servicios TICs (Infraestructura, aplicaciones, bases de datos.) ✓ Implementación de soluciones de seguridad perimetral y de antimalware ✓ Inclusión dentro del contrato de servicios TIC el borrado seguro	**Actividades realizadas durante el periodo:** -Se observa el informe de operación de servicios TICs del Proceso de Seguridad Informática respecto a vulnerabilidades -Informe de Seguridad Informática	**Primera Línea de Defensa:** La Oficina de Tecnologia y Sistemas de Información realiza los seguimientos e informes respecto a Seguridad Informática y a las vulnerabilidades encontradas por el operador *"Unión Temporal Gestión Integral MEN", para* evitar la materialización del riesgo. **Segunda Línea de Defensa:** La Subdirección de Desarrollo Organizacional realizó seguimiento sobre el adecuado diseño de los controles para la mitigación del riesgo identificado. Igualmente, se observó el seguimiento al reporte de evidencias registradas en el Sistema Integrado de Gestión-SIG

✓ Incumplimiento de las políticas de seguridad y privacidad de la información ✓ Ataques Informáticos (Virus informáticos o código malicioso, Denegación de Servicios (DoS), Phishing, inyección de código, ataques de fuerza bruta, SPAM, etc.) ✓ Acciones no autorizadas (Uso no autorizado de los equipos de cómputo o comunicaciones. Copia fraudulenta del software o sistemas de información, Uso de software no autorizado por el MEN, Corrupción de los datos, Procesamiento ilegal de datos, etc.) ✓ Validar nuevas herramientas para borrado seguro **CONTROLES:** ✓ Verificar trimestral el contrato de operación de servicios TICs - Proceso de Seguridad Informática - Plan de escaneo de vulnerabilidades / Plan de Pentesting ✓ Verificar trimestralmente los informes de seguridad emitidos por el operador de servicios TICs **EVALUACIÓN DEL RIESGO RESIDUAL:** **Riesgo Residual:** Zona de Riesgo Extremo **Acción de manejo:** Reducir el riesgo **PLAN DE ACCIÓN O DE MANEJO:** Realizar semestralmente el escaneo de vulnerabilidades y pentest a la plataforma de escritorios virtuales lo que permitirá tener un control más riguroso del manejo de los activos de información. Fecha de Inicio 1/01/2021 Fecha de Finalización: 31/12/2021 **Meta:** 1 **Porcentaje:** 100%		**Tercera Línea de Defensa:** La Oficina de Control Interno observó que el proceso monitorea el riesgo identificado. Se recomienda revisar y ajustar la matriz de riesgos del proceso de Gestión de Servicios TIC, teniendo en cuenta los cambios efectuados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5-diciembre 2020 del DAFP, en los siguientes aspectos: -Articular la institucionalidad de MIPG "Política Gobierno Digital" con la gestión del riesgo. -Ajustar la redacción del riesgo, causas y controles -Tener en cuenta la clasificación del riesgo en el momento de identificarlo. - Revisar los controles establecidos teniendo en cuenta los parámetros establecidos en la guía. - Ajustar la redacción y diseño para las causas identificadas. - Ajustar la redacción, diseño y evaluación de los controles según la calificación. -Armonizar el tratamiento de los riesgos para cumplir con los objetivos estratégicos y de proceso de la entidad.

Fuente: Matriz de riesgos de corrupción SIG-Proceso "Gestión de Servicios TIC".

En el diseño de los controles de la matriz de riesgos del Proceso de Gestión de Servicios TIC, se pudo establecer que para cada riesgo se tiene identificado el responsable de llevar a cabo la actividad de control, la periodicidad para su ejecución, el propósito de este, así como las actividades de control. En la actualidad, los riesgos de la Entidad se encuentran en proceso de actualización, de acuerdo con los lineamientos de la "Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas DAFP -V.05 diciembre 2020" del Departamento Administrativo de Función Pública.

ACTIVOS DE INFORMACIÓN Y SEGURIDAD DIGITAL

En la verificación realizada en el Sistema Integrado de Gestión-SIG, se evidenció que el Proceso de Gestión de Servicios TIC, identificó 118 activos de información, los cuales están debidamente catalogados, sin embargo, se observó que 7 activos con valor "alto" y clasificación "Información pública reservada", no se encuentran catalogados como riesgos de seguridad digital dentro del proceso, lo anterior podría generar una vulneración de la plataforma informática y de los activos de información, de acuerdo como lo indica la Guía de Administración del Riesgo-Código PM-GU-01 V.04

En cuanto a los activos de información de la Entidad, estos se han ido actualizando durante la vigencia 2021 con apoyo y acompañamiento de la Subdirección de Desarrollo Organizacional, la Oficina de Tecnología y Sistemas de la Información y los enlaces de cada dependencia, siendo publicados en el Sistema Integrado de Gestión (SIG), los cuales son insumo para la formulación e identificación de los riesgos digitales del Ministerio de Educación Nacional y del Proceso Gestión de Servicios TIC.

Para la actualización de los activos de Información se estableció un sitio en SharePoint de Seguridad Digital donde se encuentra alojado el video y presentación de las capacitaciones realizadas, a esta herramienta tienen acceso los líderes de cada área para acceder a la información cuando lo requieran.

En cuanto a los riesgos del Sistema de Gestión de Seguridad de la Información (SGSI) se tiene un plan de tratamiento que inicia en agosto de 2021 y finaliza en el mes de diciembre de 2021, dicho plan tiene como fin identificar causas y actualizar la redacción de los controles, revisión y ajuste de riesgos identificados y estado de plan de manejo.

Los incidentes de Seguridad de la Información se van a manejar y centralizar desde la herramienta de mesa de ayuda CA Service Manager, dado que el operador es el que va a realizar las acciones correspondientes, ya que no tienen acceso al módulo del SIG y no queda la trazabilidad ni las evidencias relacionadas.

PLANES, PROGRAMAS, PROYECTOS E INDICADORES:

Al revisar el avance de las metas del proceso, con corte al 30 de junio de 2021 del Plan de Acción Institucional, se evidenció el siguiente comportamiento:

Indicador	Avance corte a junio 2021	Observaciones Control Interno
122- Porcentaje de avance en la implementación del Plan de fortalecimiento de servicios tecnológicos **Medio de Verificación:** Informe de avance en la implementación del plan de fortalecimiento de servicios tecnológicos **Meta para la vigencia 2021:** 85% **Fórmula de cálculo:** Número de actividades ejecutadas del plan de fortalecimiento de servicios tecnológicos / Número total de actividades planeadas	Se observa un avance del 46%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del Plan de Fortalecimiento de Servicios Tecnológicos para la vigencia 2021, alineado a la arquitectura objetivo del Ministerio***" fue entregado en el mes de marzo de 2021. ✓ ***"Elaboración del estado actual de los servicios tecnológicos del Ministerio, a nivel de obsolescencia tecnológica o deficiencia en capacidad y rendimiento, alineado a la arquitectura objetivo del Ministerio: 1. Nodos Hiperconvergentes (almacenamiento y memoria) 2. Equipos de red. 3. Equipos***	Se observa la entrega de los hitos en el tiempo establecido. La Oficina de Tecnología y Sistemas de Información - OTSI - adelantó las siguientes actividades: ✓ Nodos Hiperconvergentes ✓ Seguridad Informática ✓ Plan de Mantenimiento Preventivo CC y equipos activos MEN, Traslado de planta telefónica MEN ✓ Adquisición licenciamiento y Capacidad requerida para operar

ESTRATEGIAS PARA MOVILIZAR LA META 1. Migración servicios no críticos a la Nube. 2. Continuar la modernización de la red LAN del Ministerio. 3. Modernización de la solución de control de acceso. 4. Reducción de riesgos de seguridad informática. 5. Diseñar e implementar nuevas modalidades de suministro de equipos de cómputo para los colaboradores del Ministerio. **Periodicidad:** Trimestral	***de cómputo y de usuario final del Ministerio. 4. Licenciamiento base***" fue entregado en el mes de abril de 2021 El hito: "***Elaboración de los anexos técnicos que soportan la necesidad de implementación del plan de servicios tecnológicos para la vigencia 2021***" está programado para entregarlo en el mes de julio de 2021. El hito: "***Desarrollo del Plan de Fortalecimiento de Servicios Tecnológicos 2021 alineado a la arquitectura objetivo del Ministerio***" está programado para entregarlo en el mes de diciembre de 2021.	La Oficina de Control Interno evidencia que se han realizado actividades establecidas en el plan de fortalecimiento, sin embargo, no se observó el total de actividades planeadas y las ejecutadas para constatar el porcentaje de avance. Se recomienda validar el avance de acuerdo con la fórmula de cálculo y continuar con las acciones pertinentes para dar cumplimiento a la meta.
334- Porcentaje de avance en la implementación del plan integral de acompañamiento a las entidades adscritas y vinculadas en TI **Medio de Verificación:** Informe de avances en la implementación del plan integral de acompañamiento **Meta para la vigencia 2021:**75% **Fórmula de cálculo:** Número de actividades ejecutadas del plan integral de acompañamiento / Número total de actividades planeadas ESTRATEGIAS PARA MOVILIZAR LA META 1. Acompañamiento en Gobierno Digital 2. Acompañamiento en Seguridad Digital 3. Apropiación de buenas prácticas de gestión **Periodicidad:** Trimestral	Se observa un avance del 50%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración versión inicial del plan integral de acompañamiento a las entidades adscritas y vinculadas en TI para la vigencia 2021***" fue entregado en el mes de marzo de 2021. ✓ ***"Elaboración del plan integral de acompañamiento a las entidades adscritas y vinculadas en TI para la vigencia 2021***" fue entregado en el mes de junio de 2021 El hito: "***Desarrollo de sesiones de acompañamiento dirigidas a las Entidades adscritas y vinculadas, orientadas a creación e implementación del Centro de respuesta a incidentes de seguridad digital (CSIRT) (Equipo de Respuesta a Incidentes de Seguridad Digital) del sector Educación e implementación de la política de gobierno digital.***" está programado para entregarlo en el mes de septiembre de 2021. El hito: "***Desarrollo de sesión de cierre al acompañamiento dirigido a las entidades adscritas y vinculadas (taller lecciones aprendidas y retos implementación CSIRT sector Educación)***" está programado para entregarlo en el mes de diciembre de 2021.	Se observa la entrega de los hitos en el tiempo establecido. La Oficina de Control Interno evidenció el plan integral de acompañamiento, sin embargo, solo se ha realizado una (1) actividad de las aproximadamente 18. No se constató el porcentaje de avance de acuerdo con la fórmula de cálculo. Se recomienda validar el avance de acuerdo con la fórmula de cálculo y continuar con las acciones pertinentes para dar cumplimiento a la meta. Se observan debilidades en los roles que ejercen la primera y segunda línea en la labor de seguimiento y monitoreo respecto a validación de controles existentes y medio de verificación para alcanzar la meta propuesta.

340- Porcentaje de avance en la implementación de la Política de Gobierno Digital **Medio de Verificación:** Informe de avance del plan de implementación de la Política de Gobierno Digital **Meta para la vigencia 2021:** 95% **Fórmula de cálculo:** Número de actividades ejecutadas del plan de implementación de la política de Gobierno Digital / Número de actividades planeadas ESTRATEGIAS PARA MOVILIZAR LA META Preparación para medición FURAG **Periodicidad:** Trimestral	Se observa un avance del 50%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del autodiagnóstico de la implementación de la política de Gobierno Digital vigencia 2021***" fue entregado en el mes de mayo de 2021. El hito: "***Elaboración del plan de implementación de la Política de Gobierno Digital vigencia 2021***" está programado para entregarlo en el mes de julio de 2021. El hito: "***Cierre de las brechas identificadas en el diagnóstico de la política de gobierno digital vigencia 2021"*** está programado para entregarlo en el mes de diciembre de 2021.	Se observa la entrega de los hitos en el tiempo establecido. La Oficina de Control Interno no pudo constatar el porcentaje de avance de acuerdo con la fórmula de cálculo, lo cual genera incertidumbre en el reporte entregado por la Oficina de Tecnologia y Sistema. Se recomienda validar el avance de acuerdo con dicha fórmula y continuar con las acciones pertinentes para dar cumplimiento a la meta. Se observan debilidades en los roles que ejercen la primera y segunda línea en la labor de seguimiento y monitoreo respecto a validación de controles existentes y medio de verificación para alcanzar la meta propuesta.
341- Porcentaje de avance en la implementación del Plan de Seguridad y Privacidad de la Información **Medio de Verificación:** Informe de avance del Plan de Seguridad y Privacidad de la Información **Meta para la vigencia 2021:** 87% **Fórmula de cálculo:** Número de actividades ejecutadas del plan de Seguridad y Privacidad de la Información / Número total de actividades planeadas ESTRATEGIAS PARA MOVILIZAR LA META 1. Generación de protocolos de paso a producción incluyendo IPv6. 2. Campaña de divulgación en Seguridad y Privacidad de la información **Periodicidad:** Trimestral	Se observa un avance del 50,8%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del autodiagnóstico del modelo de seguridad y privacidad de la información***" fue entregado en el mes de marzo de 2021. ✓ "***Validación y actualización de activos de información para 100% procesos del MEN***" fue entregado en el mes de junio de 2021. El hito: "***Actualización del plan de comunicación del Sistema de Gestión de Seguridad y Privacidad de la Información***" está programado para entregarlo en el mes de agosto de 2021. El hito: "***Validación y actualización de riesgos de seguridad de la información para 100% procesos del MEN"*** está programado para entregarlo en el mes de diciembre de 2021.	Se observa la entrega de los hitos en el tiempo establecido. La Oficina de Control Interno no pudo constatar el porcentaje de avance de acuerdo con la fórmula de cálculo. Se recomienda validar el avance de acuerdo con dicha fórmula y continuar con las acciones pertinentes para dar cumplimiento a la meta. Se observan debilidades en los roles que ejercen la primera y segunda línea en la labor de seguimiento y monitoreo respecto a validación de controles existentes y medio de verificación para alcanzar la meta propuesta.

342- Porcentaje de avance en la implementación de la Arquitectura Empresarial del Sector Educación **Medio de Verificación:** Informe de avance en la implementación de la Arquitectura Empresarial del Sector Educación **Meta para la vigencia 2021:** 40% **Fórmula de cálculo:** Número de actividades ejecutadas / Número de actividades planeadas ESTRATEGIAS PARA MOVILIZAR LA META 1. Acompañar la renovación de los servicios de información para que cumplan con la arquitectura objetivo 2. Servicios de datos implementados para los ocho (8) registros únicos. 3. Calidad sobre los datos maestros, acciones e históricos **Periodicidad:** Trimestral	Se observa un avance del 50,0%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Priorización renovación de los servicios de información para que cumplan con la arquitectura objetivo.***" fue entregado en el mes de marzo de 2021. ✓ "***Implementación de servicios de datos para los registros únicos de lugares de desarrollo de programas académicos***" fue entregado en el mes de junio de 2021. El hito: "***Implementación del plan de calidad de datos sobre los datos maestros, las acciones y los históricos para los registros únicos de Personas, Estudiantes y Pares***" está programado para entregarlo en el mes de septiembre de 2021. El hito: "***Implementación del Servicio de trazabilidad de los estudiantes graduados desde EPBM a Educación Superior"*** está programado para entregarlo en el mes de diciembre de 2021.	Se observa la entrega de los hitos en el tiempo establecido. La Oficina de Control Interno no pudo constatar el porcentaje de avance de acuerdo con la fórmula de cálculo. Se recomienda validar el avance de acuerdo dicha fórmula y continuar con las acciones pertinentes para dar cumplimiento a la meta. Se observan debilidades en los roles que ejercen la primera y segunda línea en la labor de seguimiento y monitoreo respecto a validación de controles existentes y medio de verificación para alcanzar la meta propuesta.
343- Porcentaje de avance en el fortalecimiento de los servicios de información existentes y nuevos **Medio de Verificación:** Informe de avance en el fortalecimiento de los servicios de información existentes y nuevos **Meta para la vigencia 2021:** 75% **Fórmula de cálculo:** Número de servicios de información fortalecidos / Número total de servicios de información **Periodicidad:** Trimestral	Se observa un avance del 50,0%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Definición de los proyectos de fortalecimiento de servicios de información priorizados para la vigencia 2021***" fue entregado en el mes de marzo de 2021. ✓ "***Entrega de los proyectos de fortalecimiento de servicios de información a los responsables de su ejecución (proveedores)***" fue entregado en el mes de junio de 2021. El hito: "***Elaboración de la ingeniería de análisis de los proyectos de fortalecimiento de servicios de información priorizados para la vigencia 2021***" está programado para entregarlo en el mes de agosto de 2021. El hito: "***Elaboración del diseño detallado de los requerimientos especificados para los proyectos de fortalecimiento de servicios de información priorizados para***	Se observa la entrega de los hitos, sin embargo, el hito "*Entrega de los proyectos de fortalecimiento de servicios de información a los responsables de su ejecución (proveedores)*" no cumplió con la fecha programada para entregar en el mes de mayo de 2021. La Oficina de Control Interno no pudo constatar el porcentaje de avance de acuerdo con la fórmula de cálculo. Se recomienda validar el avance de acuerdo con dicha fórmula y continuar con las acciones pertinentes para dar cumplimiento a la meta. Se observan debilidades en los roles que ejercen la primera y segunda línea en la labor de seguimiento y monitoreo respecto a validación de controles existentes y medio de

	la vigencia 2021" está programado para entregarlo en el mes de diciembre de 2021.	verificación para alcanzar la meta propuesta.
278- Número de proyectos de las Secretarías de Educación viabilizados para "Conectividad escolar en Instituciones Educativas Oficiales" **Medio de Verificación:** Informe de proyectos de conectividad escolar viabilizados **Meta para la vigencia 2021:** 85 (número) **Fórmula de cálculo:** Número de proyectos de las Secretarías de Educación viabilizados por el Programa Conexión Total para "Conectividad escolar en Instituciones Educativas Oficiales" **Periodicidad:** Trimestral	Se observa un avance del 71,8%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del plan de trabajo de la asistencia técnica a las Entidades Territoriales Certificadas para la estructuración de proyectos de conectividad***" fue entregado en el mes de marzo de 2021. ✓ "***Actualización del documento de lineamientos de conectividad escolar para las sedes educativas oficiales***" fue entregado en el mes de abril de 2021. El hito: "***Desarrollo de mesas de trabajo con las Secretarías de Educación para reforzar los lineamientos técnicos para la contratación de conectividad escolar***" está programado para entregarlo en el mes de julio de 2021. El hito: "***Consolidación de resultados de los proyectos viabilizados a las Secretarías de Educación para la contratación del servicio de conectividad escolar de las sedes educativas por parte de las entidades territoriales"*** está programado para entregarlo en el mes de diciembre de 2021.	Se observa la entrega de los hitos en el tiempo establecido. La Oficina de Tecnología y Sistemas de Información (OTSI) viabilizó 61 proyectos de conectividad de 44 Secretarías de Educación distribuidos de la siguiente manera: enero 1, febrero 3, marzo 16, abril 13, mayo 15 y junio 13. Para este indicador solicitaron el ajuste de la programación de las metas de los trimestres 2 y 3 con las nuevas proyecciones, de acuerdo con el flujo de proyectos recibidos a la fecha. La Oficina de Control Interno evidencia que se realizaron las actividades programadas en el PAI, demostrando un avance del 71,8%. Sin embargo, se recomienda continuar con las acciones pertinentes para dar cumplimiento a la meta.

Fuente: Matriz PAI 2021 Oficina de Tecnología y Sistemas de Información

En el seguimiento al Plan de Acción Institucional, se han entregado los hitos correspondientes a cada uno de los indicadores. Así mismo, se observó que el avance de los indicadores no se mide de acuerdo con la fórmula de cálculo, por lo tanto, se recomienda revisar y realizar los ajustes correspondientes con acompañamiento metodológico de la Oficina Asesora de Planeación y Finanzas.

Se observan debilidades en los roles que ejercen la primera y segunda línea en la labor de seguimiento y monitoreo respecto a validación de controles existentes y medio de verificación para alcanzar la meta propuesta.

PROCEDIMIENTO GESTIÓN DE CAPACIDAD ST-PR-03 V.4

A través de este procedimiento se planifica el crecimiento de la infraestructura, asegurando las necesidades de capacidad de los servicios de TI, lo que permite optimizar los recursos de tecnología y la disponibilidad de los recursos TI.

En el procedimiento Gestión de la Capacidad, en las disposiciones generales hacen referencia al "Operador UNE" el cual ya no se encuentra contratado por el Ministerio de Educación Nacional.

El proceso de Gestión de Servicios TIC cuenta con un plan de gestión de capacidad realizado por el operado UNIÓN TEMPORAL GESTIÓN INTEGRAL MEN en el mes de enero de 2021, de acuerdo con lo establecido en el Contrato CO1.PCCNTR.1989604. Este plan analiza el estado actual de la plataforma de Hiperconvergencia tanto del clúster de aplicaciones como de bases de datos, en cuanto a CPU, memoria, almacenamiento, seguridad informática; obteniendo el nivel de crecimiento mensual y el promedio de consumo por la vigencia 2020, con el fin de identificar las acciones que garanticen las necesidades del negocio.

El plan de gestión de capacidad es aprobado en primera instancia por la interventoría mediante un oficio radicado por el Sistema de Gestión Documental y luego es aprobado por el Gestor de Capacidad del Ministerio de Educación Nacional. Dicho plan se actualiza periódicamente, de acuerdo a las necesidades que pueden surgir mediante las actividades de los procedimientos de Gestión de solicitudes, Gestión de Incidentes, Gestión de Cambios y Gestión de la Demanda.

En las reuniones semanales de gestión técnica, se evalúan las capacidades y si se requiere realizar ajustes, estas son llevadas al comité de cambios (CAB) con el fin de evaluar la viabilidad y límites permitidos del fabricante. Una vez que se obtienen las aprobaciones necesarias, se implementa el cambio a través de un tiquete en la herramienta CA Service Desk donde se adjunta el RFC.

Para el monitoreo de la capacidad, el Ministerio de Educación Nacional cuenta con las herramientas CA Spectrum, CA Performance Management y VMware las cuales se parametrizan con la línea base, permitiendo tener las métricas de consumo y de acuerdo con los resultados se toman las acciones correspondientes.

En el Plan Estratégico de Tecnologías de la Información - PETI en el numeral "***8.2 Proyección de presupuesto área de TI"*** en la actividad *"Aumentar el nivel de capacidad de infraestructura y disponibilidad de servicios de TI"* se detalla el presupuesto para las acciones programadas en el plan de gestión de la capacidad.

Actualmente, se encuentra en proceso la Adquisición e instalación de hardware requerido para ampliación de capacidad de la infraestructura hiperconvergente propiedad del Ministerio de Educación Nacional.

Se han implementado escritorios virtuales, nubes públicas, Colombia Aprende, préstamos de equipos, doble factor de autenticación, Microsoft Teams, con el fin de mejorar la prestación del servicio TI.

De acuerdo con las actas de seguimiento a la ejecución del contrato con el operador Unión Temporal Gestión Integral, se indica que se ejecutaron varios RFC, sin embargo, no se observó la actualización del plan de capacidad con los cambios realizados, como lo expresa la actividad 24 y 25 del procedimiento.

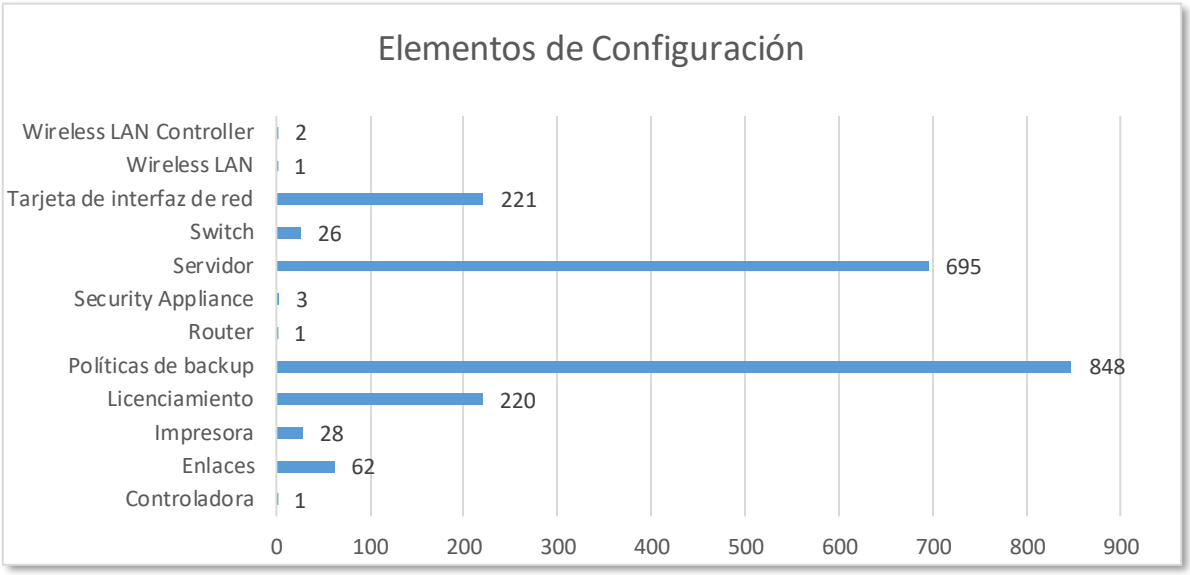
PROCEDIMIENTO GESTIÓN DE CONFIGURACIÓN ST-PR-10 V.04

El procedimiento de Gestión de la Configuración permite identificar y documentar las características funcionales y físicas de un producto, el resultado, así como un servicio o componente; controlar, registrar e informar cada cambio y su estado de implementación a lo largo de su vida útil.

El proceso cuenta con el plan de gestión de la configuración que describe la manera en que la información sobre los elementos será registrada y actualizada de modo que se mantengan consistentes y/u operando, de igual manera se lleva control mediante la herramienta CA Service Desk Manager.

El proceso de Gestión de Servicios TIC a través de la herramienta CA Service Desk Manager cuenta con la base de datos de configuración (CMDB) donde se identifican los elementos de configuración (CI) y cada una de sus características.

Actualmente se encuentran registrados 2.108 activos, configurados con la siguiente clasificación:



Fuente: CA Service Desk Manager-Equipo Auditor OCI

Una vez el plan de gestión de la configuración es aprobado, el Gestor de Cambios crea la orden en la herramienta CA, ya sea para actualización, creación o eliminación de un elemento, el gestor de la configuración verifica la información de la solicitud, confirma su completitud y si está asociada a un RFC. Una vez tienen las aprobaciones correspondientes, el operador realiza el cambio en la herramienta de monitoreo SPECTRUM y así mismo esta información se sincroniza automáticamente semanalmente con la herramienta de CA Service Desk Management.

La herramienta SPECTRUM tiene un reporte que permite identificar quien hizo el cargue o modificación, fecha de la acción y el elemento configurado. En caso de que se presente eliminación de un elemento en esa aplicación, en la herramienta CA se debe realizar la inactivación manualmente.

En el procedimiento Gestión de Configuración en la actividad 13 indica "MODIFICACIÓN ASOCIADA A UNA ORDEN DE CAMBIO", la cual si no tiene una orden de cambio "*El gestor de la configuración determinará bajo sus propios criterios y los establecidos por el MEN si la modificación solicitada se puede realizar, debido a que no hay un cambio asociado con el cual justificar la modificación de la información del CI.",* lo anterior podría ocasionar perdida de seguimiento y trazabilidad a los cambios requeridos.

Para la configuración de los elementos de licenciamiento y software se creó el documento "*Memoria técnica de Configuración Intangibles Ministerio de Educación Nacional*", este tiene como objetivo "*plasmar la información configurada para los elementos de configuración sobre la integración y control de licenciamiento y software de la CMDB en la herramienta Ca Service Desk Manager para el Ministerio de Educación Nacional. El contenido de este documento es el insumo principal para la descripción de las labores técnicas ejecutadas por el equipo de M.S.L Distribuciones y CIA durante la etapa de parametrización de la solución propuesta*", con el fin de documentar las actividades realizadas. Están en proceso de actualización las licencias de software y en pruebas los reportes para identificar la disponibilidad y la vigencia de las mismas.

En las políticas generales del procedimiento de Gestión de Configuración se indica *"Contar con un plan de auditorías realizado por el operador, para asegurar que la información registrada en la CMDB (Base de datos de la gestión de configuración), es igual a la que se encuentra en los elementos del ambiente de producción*", no se tiene específicamente un plan, sin embargo, la firma interventora realiza seguimiento semanal al CMDB y a las políticas de backup.

MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN:

La Oficina de Tecnología y Sistemas de Información realiza seguimiento a las actividades programadas a través de reuniones con el líder o supervisor y los proveedores tecnológicos, validando el avance y cumplimiento de los compromisos establecidos.

El proceso realiza control y seguimiento a las PQRSD por medio de un reporte semanal, el cual se envía a cada uno de los coordinadores de grupo indicándoles los que están pendientes de tramitar para evitar entregar respuestas extemporáneas, garantizando así la oportunidad de las mismas.

PARTICIPACION CIUDADANA:

Se evidenció, que el proceso de Servicios TIC no cuenta con acciones formuladas en el Plan de Participación Ciudadana, sin embargo, apoya esta gestión por medio de mejoras en herramientas como la página WEB para la usabilidad y accesibilidad, radicación de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias, disponibilidad tecnológica de chat (Atención al Ciudadano, Portal Colombia Aprende), cargue de datos al portal de datos.gov que son publicados después de la aprobación de los mismos; estos canales permiten la comunicación instantánea con los ciudadanos, maestros, directivos docentes y el Ministerio de Educación Nacional, entre otros.

CONCLUSIONES:

1. En el diseño de los controles de la matriz de riesgos del Proceso de Gestión de Servicios TIC, se pudo establecer que para cada riesgo se tiene identificado el responsable de llevar a cabo la actividad de control, la periodicidad para su ejecución, el propósito de este, así como las actividades de control. En la actualidad, los riesgos de la Entidad se encuentran en proceso de actualización, de acuerdo con los lineamientos de la "Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas DAFP -V.05 diciembre 2020" del Departamento Administrativo de Función Pública.

2. En el seguimiento al plan de acción institucional, se han entregado los hitos correspondientes a cada uno de los indicadores. Así mismo, se observó que el avance de los indicadores no se mide de acuerdo con la fórmula de cálculo.

3. En la verificación realizada en el Sistema Integrado de Gestión-SIG, se evidenció que el Proceso de Gestión de Servicios TIC, identificó 118 activos de información, los cuales están debidamente catalogados, sin embargo, se observó que 7 activos con valor "*alto*" y clasificación "*Información pública reservada*", no se encuentran catalogados como riesgos de seguridad digital dentro del proceso, lo anterior podría generar una vulneración de la plataforma informática y de los activos de información, de acuerdo como lo indica la *Guía de Administración del Riesgo-Código PM-GU-01 V.04, numeral 9.1. Lineamientos operativos para Mapas de Riesgos institucionales, corrupción, soborno, fraude y seguridad de la información-literal m)*

4. En la validación efectuada se observó que en las disposiciones generales hacen referencia al "Operador UNE", el cual ya no se encuentra contratado por el Ministerio de Educación Nacional.

5. En las políticas generales del procedimiento de Gestión de Configuración se indica "*Contar con un plan de auditorías realizado por el operador, para asegurar que la información registrada en la CMDB es igual a la que se encuentra en los elementos del ambiente de producción*", no se tiene específicamente un plan, sin embargo, la firma interventora realiza seguimiento semanal al CMDB y a las políticas de backup.

6. El proceso cuenta con el plan de gestión de la configuración, el cual describe la manera en que la información sobre los elementos será registrada y actualizada, de modo que se mantengan consistentes y/u operando, de igual manera se lleva control mediante la herramienta CA Service Desk Manager.

RECOMENDACIONES

1. Revisar y realizar los ajustes correspondientes a los Indicadores del Plan de Acción Institucional con acompañamiento metodológico de la Oficina Asesora de Planeación y Finanzas.

2. Validar los activos de información del Proceso de Gestión de Servicios TIC y determinar cuáles de ellos por su criticidad y clasificación deben ser catalogados e identificados como riesgo de seguridad digital.

3. Revisar el procedimiento Gestión de Capacidad ST-PR-03 V.4 y efectuar los ajustes en las disposiciones generales, citando el operador de manera genérica sin mencionar un contratista específico.

4. Revisar el procedimiento Gestión de Configuración ST-PR-10 V.4 y efectuar los ajustes que el proceso considere pertinente en la actividad 13 del mismo.

5. Contar con el Plan de auditorías, con el fin de que el operador asegure que la información registrada en la CMDB es igual a la que se encuentra en los elementos del ambiente de producción, de tal manera que se obtengan resultados de mejora continua en la ejecución del procedimiento Gestión de Configuración ST-PR-10 V.4

INFORME DETALLADO			
Resultado		**Descripción**	**Recomendación**
HZ	**OM**		
	X	**ACTIVOS DE INFORMACIÓN Y SEGURIDAD DIGITAL** En la verificación realizada en el Sistema Integrado de Gestión-SIG, se evidenció que el Proceso de Gestión de Servicios TIC, identificó 118 activos de información, los cuales están debidamente catalogados, sin embargo, se observó que 7 activos con valor "*alto*" y clasificación "*Información pública reservada*", no se encuentran catalogados como riesgos de seguridad digital dentro del proceso. Lo anterior podría generar una vulneración de la plataforma informática y de los activos de información, de acuerdo como lo indica la *Guía de Administración del Riesgo-Código PM-GU-01 V.04, numeral 9.1. Lineamientos operativos para Mapas de Riesgos institucionales, corrupción, soborno, fraude y seguridad de la información-literal m*	Validar los activos de información del Proceso de Gestión de Servicios TIC y determinar cuales de ellos por su criticidad y clasificación deben ser catalogados e identificados como riesgo de seguridad digital.

	X	**Plan de Acción Institucional** En el seguimiento al Plan de Acción Institucional, se han entregado los hitos correspondientes a cada uno de los indicadores. Sin embargo, se observó que el avance de los indicadores no se mide de acuerdo con la fórmula de cálculo.	Se recomienda revisar y realizar los ajustes correspondientes con acompañamiento metodológico de la Oficina Asesora de Planeación y Finanzas.
	X	**PROCEDIMIENTO GESTIÓN DE CAPACIDAD ST-PR-03 V.4** En la validación efectuada se observó que en las disposiciones generales hacen referencia al "Operador UNE" el cual ya no se encuentra contratado por el Ministerio de Educación Nacional.	Revisar el procedimiento Gestión de Capacidad ST-PR-03 V.4 y efectuar los ajustes respecto a la mención genérica del operador en las disposiciones generales.
	X	**PROCEDIMIENTO GESTIÓN DE CONFIGURACIÓN ST-PR-10 V.04** En las políticas generales del procedimiento de Gestión de Configuración se indica "*Contar con un plan de auditorías realizado por el operador, para asegurar que la información registrada en la CMDB es igual a la que se encuentra en los elementos del ambiente de producción*", no se tiene específicamente un plan, sin embargo, la firma interventora realiza seguimiento semanal al CMDB y a las políticas de backup. De igual manera, en la actividad 13 se indica "MODIFICACIÓN ASOCIADA A UNA ORDEN DE CAMBIO", la cual si no tiene una orden de cambio "*El gestor de la configuración determinará bajo sus propios criterios y los establecidos por el MEN si la modificación solicitada se puede realizar, debido a que no hay un cambio asociado con el cual justificar la modificación de la información del CI.",* lo anterior podría ocasionar pérdida de seguimiento y trazabilidad a los cambios requeridos.	Revisar el procedimiento Gestión de Configuración ST-PR-10 V.4 y efectuar los ajustes que el proceso considere pertinente.

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		

LÍDER DEL EQUIPO AUDITOR: Mónica Alexandra González Moreno
JEFE OFICINA DE CONTROL INTERNO: María Helena Ordóñez Burbano