Proceso: Gestión de Servicios TIC

Numero de Auditoria: 2022-G-02

Fecha Reunión de Apertura: 05 de agosto de 2022

Fecha Reunión de Cierre: 30 de diciembre de 2022

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S)

Constanza Engativá- Jefe Oficina de Tecnología y Sistemas de Información

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

- ✓ **AUDITOR LIDER**
  Mónica Alexandra Gonzalez

- ✓ **AUDITORES**
  Ingrid Bibiana Rodriguez
  Luz Yanira Salamanca

OBJETIVO DE AUDITORÍA

Verificar la eficacia de los controles y parámetros establecidos para gestionar la Seguridad de la Información y activos de información, con el propósito de retroalimentar al proceso de Gestión de Servicios TIC 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 Activos de Información Código SIG. ST-PR-16 V.01
- ✓ Procedimiento Seguridad de la información Código SIG: ST-PR-08 V.04
- ✓ Plan de Acción Institucional-PAI
- ✓ Mecanismos de Autoevaluación y Autocontrol
- ✓ Matriz de Riesgos del Proceso de Gestión, riesgos de Corrupción, riesgos de Seguridad Digital.

El periodo definido como objeto de revisión es el comprendido entre el 30 de junio de 2021 al 31 de julio de 2022.

CRITERIOS DE AUDITORÍA

-Guía para la administración del riesgo y el diseño de controles en entidades públicas-Dirección de Gestión y Desempeño Institucional DAFP-Diciembre de 2020 V. 05
-Plan de Acción Institucional PAI-Corte diciembre 2021
-Documentos existentes en el Sistema Integrado de Gestión (SIG) que se encuentran aprobados por el Ministerio de Educación Nacional, la normativa interna de la entidad, así como los criterios sobre controles aplicables que incluyen:
-Indicadores de proceso
-Procedimiento Gestión de Activos de Información ST-PR-16 V.01
-Guía Política de Gestión de Activos de Información ST-GU-23 V.01
-Procedimiento Gestión de Seguridad de la Información ST-PR-08 V.04
-Guía clasificación de la Información MEN ST-GU-17 V.01

RESUMEN GENERAL

FORTALEZAS

La Oficina de Tecnología y Sistemas de Información junto a la Oficina Asesora de Comunicaciones por medio de comunicación interna y a través del canal "RADIOMEN" realizaron sensibilización a los funcionarios y colaboradores del Ministerio mediante la campaña "Conéctate con la seguridad digital".

Semestralmente, la Oficina de Tecnología y Sistemas de Información realiza el escaneo de vulnerabilidades y pentest a la plataforma de escritorios virtuales, lo que permite tener control en el manejo de los activos de información.

RIESGOS Y EVALUACIÓN DE CONTROLES

Se realizó validación de los Riesgos de Gestión de Seguridad Digital y de Corrupción asociados al proceso de "Gestión de Servicios TIC" registrados en el Sistema Integrado de Gestión (SIG), evidenciando las siguientes situaciones:

Riesgos de Gestión

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO 1		Posibilidad de pérdida Económico y Reputacional por la No disponibilidad, integridad o confidencialidad de la información contenida en los diferentes sistemas de información debido a ataques Informáticos	**Primera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información revisó que las nuevas implementaciones estén libres de vulnerabilidades y que los sistemas de información actuales empiecen con un proceso de remediación para que también queden sin vulnerabilidades, por medio de estas validaciones, se han identificado sistemas a los que no es posible actualizar, por lo cual, se han reforzado las políticas de seguridad en los equipos de seguridad perimetral. **Segunda Línea de Defensa:** La Subdirección de Desarrollo Organizacional realizó seguimiento sobre el adecuado diseño
TIPO DE RIESGO		Seguridad digital	
IMPACTO		Económico y Reputacional	
CAUSA INMEDIATA		No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes sistemas de información	
CAUSA RAÍZ		Ataques Informáticos	
	PROBABILIDAD	MEDIA (60%)	
	IMPACTO	MODERADO (60%)	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
ANÁLISIS DEL RIESGO INHERENTE	**EVALUACIÓN ZONA DE RIESGO INHERENTE**	Zona de Riesgo MODERADA	de los controles para la mitigación del riesgo identificado. Igualmente, se observó el monitoreo al reporte trimestral registradas en el Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. **Tercera Línea de Defensa:** En la validación de las actividades relacionadas con el control reportadas en el Sistema Integrado de Gestión (SIG), se evidencian los Informes de Seguridad Informática correspondientes a los meses de abril, junio, julio de 2022, sin embargo, el informe de mayo no fue adjuntado. En dichos informes se presenta la gestión realizada a nivel de los servicios especializados de ejecución, administración y operación de seguridad informática en el Ministerio de Educación Nacional de Colombia. Se recomienda validar la descripción del control, ya que, se establece que el resultado de vulnerabilidades se presentará con periodicidad trimestral, no obstante, se observa que estos se están realizando mensualmente. Durante el periodo de seguimiento no se reportó materialización del riesgo. Dado que se mantiene en un nivel de riesgo residual Moderado, no se contempló la implementación de un plan de manejo, lo anterior de acuerdo a los lineamientos establecidos.
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	**NATURALEZA DEL CONTROL**	Preventivo	
	DEPENDENCIA	Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	El líder de seguridad valida el resultado de vulnerabilidades de manera trimestral y deja consignado el resultado en un informe	
	USUARIO(S) RESPONSABLE(S)	Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO	Preventivo (25)	
	IMPLEMENTACIÓN	Manual (15)	
	DOCUMENTACIÓN	Documentado	
	FRECUENCIA	Continua	
	EVIDENCIA	Con Registro	
	VALOR ATRIBUTOS	40%	
RIESGO RESIDUAL	**PROBABILIDAD**	BAJA (40%)	
	IMPACTO	MODERADO (60%)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo MODERADA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO 2		Posibilidad de pérdida Económico y Reputacional por la No disponibilidad, integridad o confidencialidad de la información contenida en los diferentes sistemas de información debido a fallas técnicas en los dispositivos que contienen los servidores virtuales	**Primera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información validó la disponibilidad de los equipos de Hiperconvergencia, los cuales, son los contenedores de las máquinas virtuales (sistemas de información), el resultado ha arrojado que no se están presentado inconvenientes, así mismo se han realizado las actualizaciones que la propia plataforma recomienda. **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 monitoreo al reporte trimestral registradas en el
TIPO DE RIESGO		Seguridad digital	
IMPACTO		Económico y Reputacional	
CAUSA INMEDIATA		No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes sistemas de información	
CAUSA RAÍZ		Fallas técnicas en los dispositivos que contienen los servidores virtuales	
	PROBABILIDAD	MEDIA (60%)	
	IMPACTO	CATASTRÓFICO (100%)	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
ANÁLISIS DEL RIESGO INHERENTE	**EVALUACIÓN ZONA DE RIESGO INHERENTE**	Zona de Riesgo EXTREMA	Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. **Tercera Línea de Defensa:** Se evidencia el informe de Indicadores de disponibilidad y uso por sistema de información incluyendo uso de recursos tecnológicos y uso de usuarios finales, usuarios administradores, usuarios funcionales por tipo de operación, para los meses mayo y junio de 2022, no se evidencia el mes de abril. Por otro lado, se recomienda validar la descripción del control, ya que, se establece que: ***"validan el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados relacionándolos en un acta",*** No obstante, como evidencia se están relacionando los informes de seguimiento de gestión técnica infraestructura TI. El plan de manejo está con fecha de finalización el 31 de julio de 2022. Sin embargo, al momento de la auditoria se observa un avance del 75%.
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	**NATURALEZA DEL CONTROL**	Preventivo	
	DEPENDENCIA	-Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	El líder de infraestructura y seguridad validan el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados relacionándolos en una acta	
	USUARIO(S) RESPONSABLE(S)	Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO	Preventivo (25)	
	IMPLEMENTACIÓN	Manual (15)	
	DOCUMENTACIÓN	Documentado	
	FRECUENCIA	Continua	
	EVIDENCIA	Sin Registro	
	VALOR ATRIBUTOS	40%	
RIESGO RESIDUAL	**PROBABILIDAD**	BAJA (40%)	
	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo EXTREMA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	
ACCIÓN DE MANEJO	**CONTROL**	El líder de infraestructura y seguridad validan el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados relacionándolos en una acta	
	ACCIÓN	Diseñar y Ejecutar plan de actualizaciones de acuerdo a los reportes del control	
	REGISTRO	Plan	
	RESPONSABLE	Edwar Aldemar Hidalgo Acosta / Contratista	
	INDICADOR	porcentaje de avance de las actualizaciones	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO 3		Posibilidad de pérdida reputacional y económica por omisiones o deficiencias en la prestación del servicio que ofrece el ministerio a sus grupos de valor, debido a la no disponibilidad de los servicios tecnológicos, servicios de información y plataformas.	**Primera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información aplica el control de los sistemas de información a los cuales no ha sido posible realizar actualizaciones de versión de TLS para que se puedan trabajar con las fábricas correspondientes y poder llegar a versiones actualizadas y soportadas. Así mismo, revisaron el estado de la infraestructura con el fin de validar si existe algún end of life (fin de vida) y proceder con actualización o cambio de equipo tecnológico. Se verificaron los bugs que puedan afectar los sistemas de información, no se han presentado este tipo de comportamientos en dichas verificaciones, también se validaron unos errores conocidos y se documentan para futuros casos como gestión de conocimiento. Se reviso el comportamiento de las ordenes de cambio y se han realizado recomendaciones a nivel de la operación para que los cambios sean atendidos de manera oportuna y que no se presente desviación en los tiempos de ejecución. **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 monitoreo al reporte trimestral registradas en el Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. Este riesgo se materializó en la vigencia 2021, por lo cual fue necesario realizar actualización sobre los controles y plan de manejo programado, lo anterior se realizó en el primer trimestre de la vigencia 2022 con apoyo y acompañamiento de la Subdirección de Desarrollo Organizacional. **Tercera Línea de Defensa:** Se evidenciaron los informes de seguimiento de gestión técnica
TIPO DE RIESGO		Fallas tecnológicas	
IMPACTO		Económico y Reputacional	
CAUSA INMEDIATA		Omisiones o deficiencias en la prestación del servicio que ofrece el ministerio a sus grupos de valor.	
CAUSA RAÍZ		No disponibilidad de los servicios tecnológicos, servicios de información y plataformas.	
ANÁLISIS DEL RIESGO INHERENTE	PROBABILIDAD	MUY BAJA (20%)	
	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACIÓN ZONA DE RIESGO INHERENTE	Zona de Riesgo EXTREMA	
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	NATURALEZA DEL CONTROL	Preventivo	
	DEPENDENCIA	Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	• Los líderes de línea (aplicaciones, infraestructura y seguridad) mantendrán el inventario de casos de imposibilidad de acceso a nuevas versiones requeridas para remediar falencias, incluyendo acciones y resultados de manera trimestral. • Los lideres de linea (aplicaciones, infraestructura y seguridad) realizan seguimiento semestral de los end of life y de los end of support de los componentes tecnológicos • Los lideres de linea (aplicaciones, infraestructura y seguridad) realizaran seguimiento a los bug que puedan tener los sistemas de información. • El lider de seguridad valida de manera trimestral el cumplimiento en la efectividad de los RFC (fallidos, rollback, ejecuciones fuera de tiempo) y realiza sesiones de toma de conciencia para que este tipo de error humano no se vuelvan a presentar documentadas en un informe.	
	USUARIO(S) RESPONSABLE(S)	• Felix Fernando Vargas Villegas / Asesor • Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO	Preventivo (25)	
	IMPLEMENTACIÓN	Manual (15)	
	DOCUMENTACIÓN	Documentado	
	FRECUENCIA	Continua	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
	EVIDENCIA	Sin Registro (1 control), Sin registro (2 Control), Sin Registro (3 Control), Con registro (4 Control).	Infraestructura TI para abril, mayo y junio de 2022. Sin embargo, no se evidencia el seguimiento semestral, tal como se describe en el control. Si bien es cierto se evidenciaron los informes de seguimiento de gestión técnica Infraestructura TI, se identificó que se presenta como soporte el informe correspondiente al periodo de junio de la vigencia 2021 y no de 2022. Se evidenciaron los Informes de Cumplimiento de ANS para los meses de abril, mayo y junio de 2022, donde se analizaron los resultados de los indicadores de Nivel de Servicio. se realizó el seguimiento a la prestación y disponibilidad de los servicios ofrecidos al Ministerio de Educación Nacional, así como la medición a la calidad de los servicios prestados a la entidad. Se recomienda validar la periodicidad del control: "***Los lideres de línea (aplicaciones, infraestructura y seguridad) realizan seguimiento semestral de los end of life y de los end of support de los componentes tecnológicos"*** ya que el control establece seguimientos con periodicidad trimestral, no obstante, se están reportando de manera mensual por medio del operador. Así mismo, validar las actividades de los controles asociados a este riesgo, dado que son las mismas contempladas en el plan de manejo del riesgo. Durante el periodo de auditoria no se evidenció materialización del riesgo. La dependencia registró el avance de las actividades planteadas en el plan de manejo definido.
	VALOR ATRIBUTOS	40%	
RIESGO RESIDUAL	**PROBABILIDAD**	MUY BAJA (20%)	
	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo EXTREMA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	
ACCIÓN DE MANEJO	**CONTROL**	• Los lideres de linea (aplicaciones, infraestructura y seguridad) realizan seguimiento semestral de los end of life y de los end of support de los componentes tecnológicos • Los líderes de linea (aplicaciones, infraestructura y seguridad) mantendrán el inventario de casos de imposibilidad de acceso a nuevas versiones requeridas para remediar falencias, incluyendo acciones y resultados de manera trimestral, • -Los lideres de linea (aplicaciones, infraestructura y seguridad) realizaran seguimiento a los bug que puedan tener los sistemas de información. • -El lider de seguridad valida de manera trimestral el cumplimiento en la efectividad de los RFC (fallidos, rollback, ejecuciones fuera de tiempo) y realiza sesiones de toma de conciencia para que este tipo de error humano no se vuelvan a presentar documentadas en un informe	
	ACCIÓN	• Diseñar y ejecutar plan de actualización tecnológico de acuerdo a los end of life que se identifiquen. • Diseñar y Ejecutar actividades de subsanación de acuerdo con los hallazgos del informe. • Diseñar y ejecutar plan de actualización tecnológico de acuerdo a los bug que se identifiquen. • Realizar sesiones de sensibilización con respecto a la importancia de los roles de cada persona al momento de ejecutar un cambio.	
	REGISTRO	• Plan de actualización tecnológico • 2 Informes • Plan de actualización tecnológico • acta	
	RESPONSABLE	Edwar Aldemar Hidalgo Acosta / Contratista	
	INDICADOR	• Plan de actualización tecnológico ejecutado sobre el programado • Informe de Actividades de subsanación ejecutadas sobre las programadas • Plan de actualización tecnológico ejecutado sobre el programado • 1	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO 4		Posibilidad de pérdida Económico y Reputacional por la No disponibilidad, integridad y confidencialidad de la información contenida en los equipos de cómputo debido a hurto de activos	**Primera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información efectuó seguimiento al funcionamiento de la herramienta DLO, con la cual se realizan los backup de los usuarios finales. Por otro lado, revisaron los sitios web por los que están navegando los usuarios y a pesar de que son conexiones bloqueadas, se informa al usuario que desde el equipo está tratando de navegar a sitios no permitidos y de esta manera se recomienda que se haga un uso responsable de los recursos tecnológicos del Ministerio cuando está fuera de la entidad, para evitar acceder a un posible sitio malicioso. **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 monitoreo al reporte trimestral registrados en el Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. **Tercera Línea de Defensa:** Se evidencia Informe de Seguridad Informática correspondiente a los meses de abril y junio 2022. Sin embargo, el informe de mayo no fue adjuntado. En dichos informes se presenta la gestión realizada a nivel de los servicios especializados de ejecución, administración y operación de seguridad informática en el Ministerio de Educación Nacional, Así como, las políticas de filtrado de contenido configuradas en el FortiGate tienen diferentes restricciones de navegación para los usuarios, definidas por la entidad. Durante el periodo de seguimiento no se reportó materialización del riesgo. Dado que se mantiene en un nivel de riesgo residual Moderado, no se contempló la implementación de un plan de manejo, lo anterior de acuerdo a los lineamientos establecidos.
TIPO DE RIESGO		Seguridad digital	
IMPACTO		Económico y Reputacional	
CAUSA INMEDIATA		No disponibilidad, integridad y confidencialidad de la información contenida en los equipos de computo	
CAUSA RAÍZ		hurto de activos	
ANÁLISIS DEL RIESGO INHERENTE	**PROBABILIDAD**	MUY BAJA (20%)	
	IMPACTO	MODERADO (60%)	
	EVALUACIÓN ZONA DE RIESGO INHERENTE	Zona de Riesgo MODERADA	
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	**NATURALEZA DEL CONTROL**	Preventivo	
	DEPENDENCIA	Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	• El líder de infraestructura valida el reporte de backup de los equipos de usuario final con soporte en actas que se realizan con la interventoría • El líder de seguridad valida de manera mensual los sitios WEB a los que acceden los usuarios registrándolo en un informe	
	USUARIO(S) RESPONSABLE(S)	Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO	Preventivo (25)	
	IMPLEMENTACIÓN	Manual (15)	
	DOCUMENTACIÓN	Documentado	
	FRECUENCIA	Continua, Aleatoria	
	EVIDENCIA	Sin registro	
	VALOR ATRIBUTOS	40%	
RIESGO RESIDUAL	**PROBABILIDAD**	MUY BAJA (20%)	
	IMPACTO	MODERADO (60%)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo MODERADA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	

RIESGO IDENTIFICADO			**OBSERVACIONES OCI**
RIESGO 5		Posibilidad de pérdida Económico y Reputacional por la pérdida de la integridad, confidencialidad y no disponibilidad de la información contenida en los diferentes sistemas de información, debido a fallas técnicas en los dispositivos de seguridad	**Primera Línea de Defensa:** La Oficina de Tecnologia y Sistemas de información realizó el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs. **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 monitoreo al reporte trimestral registrados en el Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. **Tercera Línea de Defensa:** Se evidencia Informe de Seguridad Informática correspondiente a los meses de abril y junio 2022. Sin embargo, el informe de mayo no fue adjuntado. Para el periodo de auditoría, no se observan las actas que se desarrollaron con la interventoría tal como lo establece el control. Se recomienda validar el medio de verificación del control, para presentar las evidencias correspondientes del mismo. Durante el periodo de evaluación no se reportó materialización del riesgo. La dependencia registró el avance de las actividades planteadas en el plan de manejo.
TIPO DE RIESGO		Seguridad digital	
IMPACTO		Económico y Reputacional	
CAUSA INMEDIATA		No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes sistemas de información	
CAUSA RAÍZ		Fallas técnicas en los dispositivos de seguridad	
ANÁLISIS DEL RIESGO INHERENTE	**PROBABILIDAD**	BAJA (40%)	
	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACIÓN ZONA DE RIESGO INHERENTE	Zona de Riesgo EXTREMA	
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	**NATURALEZA DEL CONTROL**	Preventivo	
	DEPENDENCIA	Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	El líder de seguridad valida el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados dejando registros en actas.	
	USUARIO(S) RESPONSABLE(S)	Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO	Preventivo (25)	
	IMPLEMENTACIÓN	Manual (15)	
	DOCUMENTACIÓN	Documentado	
	FRECUENCIA	Continua	
	EVIDENCIA	Sin registro	
	VALOR ATRIBUTOS	40%	
RIESGO RESIDUAL	**PROBABILIDAD**	BAJA (40%)	
	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo EXTREMA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	
ACCIÓN DE MANEJO	**CONTROL**	-El líder de seguridad valida el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados dejando registros en actas.	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
	ACCIÓN	Diseñar y Ejecutar plan de actualizaciones de acuerdo a los reportes del control para los equipos de seguridad	
	REGISTRO	Informe	
	RESPONSABLE	Edwar Aldemar Hidalgo Acosta / Contratista	
	INDICADOR	porcentaje de avance en el plan de actualización de los equipos de seguridad	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO 6		Posibilidad de pérdida Económica y Reputacional por la No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes sistemas de información, debido a fallas técnicas en los dispositivos de comunicaciones.	**Primera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información realizó seguimiento al estado actual de los equipos de conectividad y producto de unos hallazgos se generó un plan de trabajo para remediación para que los dispositivos no tengan vulnerabilidades y por ende no vayan a afectar el servicio de conectividad al Ministerio de Educación Nacional. **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 monitoreo al reporte trimestral registradas en el Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. **Tercera Línea de Defensa:** Se evidencia Informe de Seguridad Informática correspondiente a los meses de abril y junio 2022, sin embargo, el informe de mayo no fue adjuntado. No se observan las actas que se desarrollan con la interventoría tal como lo establece el control. Se recomienda validar el medio de verificación del control, para presentar las evidencias correspondientes del mismo. Durante el periodo de seguimiento no se reportó materialización del riesgo. La dependencia registró el avance de las actividades planteadas en el plan de manejo.
TIPO DE RIESGO		Seguridad digital	
IMPACTO		Económico y Reputacional	
CAUSA INMEDIATA		No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes sistemas de información	
CAUSA RAÍZ		bug sobre las plataformas	
ANÁLISIS DEL RIESGO INHERENTE	**PROBABILIDAD**	BAJA (40%)	
	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACIÓN ZONA DE RIESGO INHERENTE	Zona de Riesgo EXTREMA	
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	**NATURALEZA DEL CONTROL**	Preventivo	
	DEPENDENCIA	Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	El líder de seguridad valida el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados dejando registros en actas	
	USUARIO(S) RESPONSABLE(S)	Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO	Preventivo (25)	
	IMPLEMENTACIÓN	Manual (15)	
	DOCUMENTACIÓN	Documentado	
	FRECUENCIA	Continua	
	EVIDENCIA	Sin registro	
	VALOR ATRIBUTOS	40%	
	PROBABILIDAD	BAJA (40%)	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO RESIDUAL	IMPACTO	CATASTRÓFICO (100%)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo EXTREMA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	
ACCIÓN DE MANEJO	CONTROL	El líder de seguridad valida el informe de disponibilidad de los dispositivos y actualizaciones que sugieran los fabricantes por bugs identificados dejando registros en actas	
	ACCIÓN	Plan de actualización tecnológica de los dispositivos de comunicaciones	
	REGISTRO	informe	
	RESPONSABLE	Edwar Aldemar Hidalgo Acosta / Contratista	
	INDICADOR	porcentaje de avance de la actualización tecnológica	

RIESGO DE CORRUPCION

RIESGO IDENTIFICADO			OBSERVACIONES OCI
RIESGO		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.	**Primera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información realizó seguimiento a las vulnerabilidades de los sistemas de información y que estos cuenten con ciertos niveles de madurez para permitir una auditoria a cualquier evento que se pueda presentar y que afecte la información contenida en los sistemas de información del Ministerio de Educación Nacional. **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 monitoreo al reporte trimestral registrados en el Sistema Integrado de Gestión-SIG de acuerdo a las fechas establecidas en la Circular 10 del 4 de marzo de 2022. **Tercera Línea de Defensa:** La Oficina de Tecnología y Sistemas de Información reporta el monitoreo del control para este periodo. Sin embargo, durante el monitoreo del segundo trimestre no presentó adjunto que dé cuenta de las actas del seguimiento a la operación de manera semanal como se define en el control. Se evidenció el Informe de Seguridad Informática correspondiente a los meses de
TIPO DE RIESGO		Corrupción	
IMPACTO		CATASTRÓFICO (20)	
ANÁLISIS DEL RIESGO INHERENTE	PROBABILIDAD	RARA VEZ (1)	
	IMPACTO	CATASTRÓFICO (20)	
	EVALUACIÓN ZONA DE RIESGO INHERENTE	Zona de Riesgo EXTREMA	
	OPCIONES DE MANEJO DEL RIESGO	Reducir el riesgo	
VALORACIÓN DEL RIESGO	NATURALEZA DEL CONTROL	Preventivo	
	DEPENDENCIA	-Oficina de Tecnología y Sistemas de Información	
	DESCRIPCIÓN DEL CONTROL	• El líder de seguridad informática verifica y realiza seguimiento semanalmente al contrato de operación de servicios TICs, los procesos de Seguridad informática, el Plan de escaneo de vulnerabilidades y Plan de Pentesting entregado por el operador, generando actas de las sesiones de trabajo realizadas. • El líder de seguridad informática verifica trimestralmente los informes de seguridad emitidos por el operador de servicios TICs y genera el plan de	

RIESGO IDENTIFICADO			OBSERVACIONES OCI
		mitigación con respecto a lo encontrado en el informe.	abril y junio 2022. Sin embargo, el informe de mayo no fue adjuntado. En los informes se reporta la socialización del plan de vulnerabilidades. El riesgo no se materializó en el periodo evaluado, se evidenció el registro del avance de las actividades del plan de manejo.
	USUARIO(S) RESPONSABLE(S)	Edwar Aldemar Hidalgo Acosta / Contratista	
	TIPO		
	IMPLEMENTACIÓN		
	DOCUMENTACIÓN		
	FRECUENCIA		
	EVIDENCIA		
	VALOR ATRIBUTOS		
RIESGO RESIDUAL	**PROBABILIDAD**	RARA VEZ (1)	
	IMPACTO	CATASTRÓFICO (20)	
	EVALUACION ZONA RIESGO RESIDUAL	Zona de Riesgo EXTREMA	
	OPCIONES MANEJO DEL RIESGO	Reducir el riesgo	
ACCIÓN DE MANEJO	**CONTROL**	El líder de seguridad informática verifica trimestralmente los informes de seguridad emitidos por el operador de servicios TICs y genera el plan de mitigación con respecto a lo encontrado en el informe.	
	ACCIÓN	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.	
	REGISTRO	Informes del Operador de servicios TICs donde se incluye esta actividad.	
	RESPONSABLE	Edwar Aldemar Hidalgo Acosta / Contratista	
	INDICADOR	Número de escaneo de Vulnerabilidades y pentest de la plataforma de escritorios virtuales ejecutados sobre Número de escaneo de Vulnerabilidades y pentest de la plataforma de escritorios virtuales programado	

Fuente: Sistema Integrado de Gestión (SIG)-Modulo riesgos

En el último trimestre de la vigencia 2021, se registró la materialización de un riesgo por indisponibilidad a nivel de datos en el sistema HUMANO y SIMAT, no se pudo restablecer de manera pronta dichos sistemas de Información, toda vez que no se contaba con una copia de seguridad disponible durante el proceso de restauración, presentando inconvenientes e involucrando a los fabricantes.

Por lo anterior, la Oficina de Tecnologia y Sistemas de Información inició un proceso de incumplimiento de ANS al operador UT.

Por lo anterior, fue necesario realizar actualización sobre los controles y plan de manejo programado, lo anterior se realizó durante el primer trimestre de la vigencia 2022 con apoyo y acompañamiento de la Subdirección de Desarrollo Organizacional.

En términos generales se puede determinar:

- Las actividades de los controles, capacitaciones se programaron a julio dado que para esa fecha estaba la operación. (No reportan los adjuntos, lista de asistencia y presentación).
  RTA OTSI: *Las evidencias fueron cargadas por la ing Clara Robayo quien manifestó en varias oportunidades que la información no estaba apareciendo.*
- El control identificado en el riesgo evaluado "lideres de línea realiza seguimiento a los Bug" presenta un informe con corte a junio de 2021 que no corresponde al periodo evaluado por la dependencia.
- En el caso del control "El líder valida trimestral los RFC" la Oficina de Control Interno sugiere verificar la periodicidad, ya que no se identificó evidencia de toma de conciencia, informe, ni actas.
- Para el control "El líder valida el resultado de vulnerabilidades" se recomienda validar si se va a presentar un informe o el medio de verificación a registrar en el SIG.

ACTIVOS DE INFORMACIÓN

En la verificación realizada en el Sistema Integrado de Gestión (SIG), se evidenció que el Proceso Gestión Servicios TIC en la vigencia 2022 cuenta con 126 activos de información identificados, los cuales están debidamente clasificados como Información pública, Información pública clasificada e Información pública reservada, con un nivel de criticidad media y alto, respectivamente; los cuales son insumo para la formulación e identificación de los riesgos digitales del Ministerio de Educación Nacional.

Total de Activos de información	**126**
Valor de activo alto con clasificación de Información Pública Reservada	6
Valor de activo medio	120
Información Pública	10
Información Pública Clasificada	35
Información Pública Reservada	75

Fuente: Sistema Integrado de Gestión-Módulo SGSI

De acuerdo con lo anterior, se validó dicha información donde se determinó que el proceso de Gestión de Servicios TIC tiene identificado los riesgos de seguridad digital para 5 de los 6 activos con valor Alto, clasificados como Información Pública Reservada.

I	Activo de la información	Descripción del activo
247	Servicios TIC (Software, Hardaware, Sistemas de	Servicios TIC (Software, Hardaware, Sistemas de
300	Equipos de computo	Infraestructura (pcs, portatiles, telefonos, impresoras, escaneres, etc)
332	Hiperconvergencia	Infraestructura de hardware para el alojamiento de soluciones
352	Dispositivos de comunicaciones	Dispositivos de comunicaciones como (stiwch, router, balanceadores, etc)
353	Dispositivos de seguridad	Dispositivos de comunicaciones como (firewall, waf, ise etc)
365	Servidores Virtuales	Infraestructura de servidores virtualizados para las operaciones TICs del MEN

Fuente: Matriz Activos Información Proceso Servicios TIC-Aplicativo SIG Modulo SGSI

PROCESO		OBJETIVO DEL PROCESO	IDENTIFICACIÓN DEL RIESGO			
			CAUSA INMEDIATA	CAUSA RAÍZ	RIESGO	TIPO DE RIES
GESTIÓN DE SERVICIOS TIC	Servidores Virtuales	Gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para la Entidad y el sector educación, mediante la adopción del marco legal para el estado colombiano en materia de TIC, con el fin de	No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes sistemas de información	Ataques Informáticos	Posibilidad de perdida Económico y Reputacional por la No disponibilidad, integridad o confidencialidad de la información contenida en los diferentes sistemas de información debido a ataques Informáticos	Seguridad digital
GESTIÓN DE SERVICIOS TIC	Hiperconvergencia	Gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para la	No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes	Fallas técnicas en los dispositivos que contienen las servidores virtuales	Posibilidad de perdida Económico y Reputacional por la No disponibilidad, integridad o confidencialidad de la	Seguridad digital
GESTIÓN DE SERVICIOS TIC	Equipos de computo	Gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para la Entidad y el sector educación, mediante la	No disponibilidad, integridad y confidencialidad de la información contenida en los equipos de computo	hurto de activos	Posibilidad de perdida Económico y Reputacional por la No disponibilidad, integridad y confidencialidad de la información contenida en los equipos de	Seguridad digital
GESTIÓN DE SERVICIOS TIC	Dispositivos de seguridad	Gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para la	No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes	Fallas técnicas en los dispositivos de seguridad	Posibilidad de perdida Económico y Reputacional por la pérdida de la integridad, confidencialidad y no	Seguridad digital
GESTIÓN DE SERVICIOS TIC	Dispositivos de comunicaciones	Gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para la	No disponibilidad, integridad y confidencialidad de la información contenida en los diferentes	bug sobre las plataformas	Posibilidad de perdida Económica y Reputacional por la No disponibilidad, integridad y confidencialidad de la	Seguridad digital

Fuente: Matriz Riesgo Gestión- Aplicativo SIG Módulo SGSI

En cuanto a los activos de información de la Entidad, estos se han ido actualizando durante la vigencia 2022 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) Modulo “SGSI”.

PLANES, PROGRAMAS, PROYECTOS E INDICADORES

Al revisar el avance de las metas del proceso, con corte al 31 de julio de 2022 del Plan de Acción Institucional, se evidenció el siguiente comportamiento:

Indicador	Avance corte a julio 2022	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 2022:** 100% **Fórmula de cálculo:** Número de actividades ejecutadas del plan de fortalecimiento de servicios tecnológicos / Número total de actividades planeadas 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	Se observa un avance 92,50%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del Plan de Fortalecimiento de Servicios Tecnológicos para la vigencia 2022, alineado a la arquitectura objetivo del Ministerio***" fue entregado en el mes de enero de 2022. ✓ ***"Elaboración del diagnóstico 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 de cómputo y de usuario final del Ministerio. 4. Licenciamiento base***" fue entregado en el mes de abril de 2022. El hito: "***Desarrollo o ejecución del Plan de Fortalecimiento de Servicios Tecnológicos para el cuatrienio alineado a la arquitectura objetivo del Ministerio***" está programado para entregarlo en el mes de diciembre de 2022.	En verificación realizada a los hitos formulados, se observó la documentación correspondiente y fueron entregados en las fechas programadas. Se observó el plan de fortalecimiento donde se definen los servicios de Gestión Técnica, Mesa de Servicios, y Seguridad Informática. Sin embargo, se realizaron actividades que no están relacionadas en dicho plan. Dado que los planes son dinámicos, se recomienda actualizarlo de acuerdo con actividades que se vayan a realizar. Así mismo, establecer las acciones correspondientes para cumplir con la meta establecida.
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 2022:** 100%	Se observa un avance 91,30%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del Plan integral de acompañamiento a las entidades adscritas y vinculadas en TI para la vigencia 2022***" fue entregado en el mes de marzo de 2022. ✓ ***"Desarrollo de sesiones de acompañamiento dirigidas a las Entidades adscritas y vinculadas, en temas de***	En verificación realizada a los hitos formulados, se observó la documentación correspondiente y fueron entregados en las fechas programadas. Se observó el plan integral de acompañamiento a las entidades adscritas y vinculadas en TI donde se definen las actividades hasta noviembre de 2022. Se encuentran los dos informes trimestrales de avance de la

Indicador	Avance corte a julio 2022	Observaciones Control Interno
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	***gobierno y seguridad digital***" fue entregado en el mes de junio de 2022 El hito: "***Elaboración de informe de cierre de cuatrienio del acompañamiento a las EAVs en Gobierno y Seguridad Digital***" está programado para entregarlo en el mes de diciembre de 2022.	implementación del Plan Integral. En el informe del segundo trimestre realizado por la Universidad EAAFIT, indican en el numeral "8. EVIDENCIAS DE SESIONES ADELANTADAS 2022", las evidencias que son parte integral del informe. Sin embargo, no se adjuntan al PAI, se recomienda sean anexadas al mismo. Adicionalmente, estas no solo deben ser soportadas con las presentaciones, sino también con los listados de asistencia o actas. El avance a julio se encuentra dentro de la meta proyectada, se recomienda continuar con las acciones correspondientes para cumplir con la meta establecida.
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 2022:** 100% **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 99,40%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del plan de implementación de la Política de Gobierno Digital vigencia 2022***" fue entregado en el mes de marzo de 2022. ✓ "Elaboración del autodiagnóstico y plan de cierre de brechas de la implementación de la política de Gobierno Digital vigencia 2022" fue entregado en el mes de julio de 2022. El hito: "***Cierre de las brechas identificadas en el diagnóstico de la política de gobierno digital para el cuatrienio"*** está programado para entregarlo en el mes de diciembre de 2022.	En verificación realizada a los hitos formulados se observó la documentación correspondiente y fueron entregados en las fechas programadas. El avance a julio se encuentra dentro de la meta proyectada, se recomienda continuar con las acciones correspondientes para cumplir con la meta establecida.
341- Porcentaje de avance en la implementación del Plan de Seguridad y Privacidad de la Información **Medio de Verificación:**	Se observa un avance 88%. De los hitos formulados en el indicador se dio el cumplimiento a: ✓ "***Elaboración del Plan de Seguridad y Privacidad de la***	En verificación realizada a los hitos formulados se observó la documentación correspondiente y fueron entregados en las fechas programadas.

Indicador	Avance corte a julio 2022	Observaciones Control Interno
Informe de avance del Plan de Seguridad y Privacidad de la Información **Meta para la vigencia 2022:** 90% **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:** Mensual	***Información para la vigencia 2022***" fue entregado en el mes de enero de 2022. ✓ "***Elaboración del autodiagnóstico del modelo de seguridad y privacidad de la información para la vigencia 2022***" fue entregado en el mes de marzo de 2022. ✓ "**Validación y actualización de activos de información para el 100% de los procesos del MEN**" fue entregado en el mes de junio de 2022. El hito: "***Validación y actualización de riesgos de seguridad de la información para 100% procesos del MEN para vigencia 2022"*** está programado para entregarlo en el mes de diciembre de 2022.	Se observó un avance del 88% para el cuatrienio. Sin embargo, el avance a julio de la vigencia 2022, es del 34%, el cual se encuentra por debajo de la meta programada del 54,5%. Se recomienda establecer las acciones necesarias para cumplir con la meta establecida.

Fuente. Plan de Acción Institucional-PAI 2022

PROCEDIMIENTO GESTIÓN DE ACTIVOS DE INFORMACIÓN ST-PR-16 V.01

En la revisión realizada se observó que la Oficina de Tecnologías y Sistemas de Información mediante la comunicación 2022-IE-015958 del 18 de abril de 2022, solicitó a las dependencias la asignación de dos colaboradores como enlaces para la identificación de activos de información para la valoración de riesgos.

Posteriormente, la Oficina de Tecnologia y Sistemas de Información realizó el 27 de mayo de 2022 una capacitación donde se trataron los siguientes temas:

- ✓ Definición de los activos de información
- ✓ Aspectos generales del procedimiento de Gestión de Activos de Información y la guía clasificación de la Información
- ✓ Compromiso para revisar el inventario de Activos de Información

Para la actividad de actualización de los activos, la Oficina de Tecnologia y Sistemas de Información creó un sitio en SharePoint donde los enlaces consultan el video de la capacitación, la presentación, los documentos asociados y el archivo de Excel con los activos de información para su verificación cuando lo requieran. Durante la auditoria, se encuentra en proceso de actualización de la información de acuerdo con los ajustes realizados por las áreas, esto de acuerdo a que se debe validar y actualizar por lo menos una vez al año.

En el procedimiento Gestión de Activos de Información, la actividad "Determinar viabilidad de la actualización de los activos de información" indica "Revisar que la solicitud de actualización de activos sea pertinente, de acuerdo con los lineamientos externos establecidos por MINTIC, los lineamientos internos establecidos por el MEN y la clasificación contenida en las Tablas de Retención Documental (TRD) vigentes para el respectivo período y el marco regulatorio aplicable al activo"; esta actividad se realiza con la Subdirección de Desarrollo Organizacional. Sin embargo, el procedimiento indica que los responsables de realizarla son el "responsable de Seguridad de la Información – OTSI y Coordinador del Grupo de Gestión Documental (Unidad de Atención al Ciudadano)".

En la Guía clasificación de la Información ST-GU-17 en su versión 1, de acuerdo con la normatividad vigente, el MEN definió los roles relacionados con la gestión de activos de información de la siguiente manera:
- Responsable de la producción de información - Productor.
- Responsable o custodio de la Información, encargado del control - Custodio.
- Técnico.
- Responsable de seguridad de la información – Seguridad
- Jurídico.
- Gobierno Digital.
- Aprobador.

Al realizar la validación del rol del jurídico a través de la Oficina Asesora Jurídica, no se evidenció que se haya tenido acompañamiento de concepto u orientaciones sobre los datos que son susceptibles de poner a disposición de cualquier individuo, tal como se establece en la Guía.

Actualmente, se encuentra en ejecución la actividad de etiquetado de los activos de información de acuerdo con el esquema de clasificación de Confidencialidad, Integridad y Disponibilidad.

En el SIG, en el módulo de SGSI, se pueden consultar los activos de información. Adicionalmente, se pueden validar las modificaciones realizadas a los activos, mediante el reporte control de cambios de estos. Sin embargo, este reporte no identifica el activo en caso de ser eliminado.

De acuerdo con la actividad 3 **ACTUALIZAR Y PUBLICAR LOS ACTIVOS DE INFORMACION,** se debe realizar la actualización de los activos de información solicitados por el líder del proceso, en el módulo SGSI del aplicativo SIG, para que se encuentren disponibles para consulta y uso de la Entidad. Así mismo, realizar la solicitud a la Oficina Asesora de Comunicaciones de publicación en el enlace de transparencia y acceso a la información pública, específicamente en el ítem 10. Instrumentos de la Gestión de la Información Pública. Se observa en la página web del Ministerio de Educación Nacional se encuentra la publicación de los activos de información en el ítem señalado con fecha del 22 de febrero de 2022, no obstante, conforme al acta del Comité de Gestión y Desempeño los activos de información fueron aprobados el 18 de mayo de 2022.
RTA OTSI: ***Para esta fecha no se tenía completada la identificación de activos para la vigencia 2022, los resultados mostrados en el comité corresponden al trabajo realizado en la vigencia 2021, el 5 de julio de 2022 se le pidió a la SDO actualizar los activos con la información recopilada.***

PROCEDIMIENTO SEGURIDAD DE LA INFORMACIÓN ST-PR-08 V.04

La Oficina de Tecnología de Sistemas de Información realizó en febrero de 2022 el autodiagnóstico, mediante el "Instrumento de Evaluación MSPI" herramienta que fue creada por el Ministerio de

Tecnologías de la Información y las Comunicaciones, con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, el cual se observó que el estado de la gestión y adopción de controles técnicos y administrativos para el MEN se encuentra en un 87%.

En la página web se publicaron el 29 de enero de 2022 los documentos “Plan Tratamiento de Riesgos de Seguridad y Privacidad de Información” y “Plan Seguridad y Privacidad de la Información”.

En la actividad 3 del procedimiento indica “APROBACIÓN DEL AUTODIAGNOSTICO Y LOS PLANES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN” en el Comité Institucional de Gestión y Desempeño del 20 de mayo de 2022, la Oficina de Tecnologia y Sistemas de Información presentó el avance del SGSS, avance de indicadores, resultado de las socializaciones, entre otros temas.

Se contempla un autodiagnóstico, por medio del cual la Oficina de Tecnologia y Sistemas de información estableció las siguientes actividades:

- Una vez creada la Guía - Política Control de Acceso ST-GU-1, se encuentra en proceso de creación del procedimiento Gestión de accesos e identidades.
- Creación de la Guía para despliegue de Servicio de Análisis Forense Digital ST-GU-22 publicada el 09 de agosto de 2022.
- Elaboración del Instructivo Lineamiento Activos de Software ST-IN-05 publicado el 03 de marzo de 2022
- Para la continuidad del negocio se está implementando el Disaster Recovery Plan (DRP) es un procedimiento que busca proteger los procesos de negocio críticos de la Entidad en el caso de que algún desastre afecte al datacenter, el cual se encuentra en proceso de validación de la información por parte de los líderes de 7 aplicaciones de 10 seleccionadas.
- Control de acceso biométrico está en diseño, el cual finaliza en diciembre 2022
- Protocolo de entrega de productos, seguridad en los proyectos
- Implementación de Privileged Access Management (PAM) que es una solución de seguridad de identidad que ayuda a proteger las organizaciones contra las ciberamenazas al supervisar, detectar y evitar el acceso con privilegios no autorizado a recursos críticos.
- Licitación nuevos nodos paras Bases de Datos.

Para el reporte de incidentes de seguridad se creó un módulo en el aplicativo de mesa de ayuda con el fin de llevar un registro y su seguimiento, a la fecha no hay operatividad en el aplicativo SIG respecto a este módulo SGSI, llevándose a cabo por medio del aplicativo de mesa de ayuda de tecnología.

Respecto a la declaración de aplicabilidad, la Oficina de Tecnologia y Sistemas de Información maneja la información de sus controles, en una matriz donde identifican si esta implementado y su medio soporte, evidenciando que se encuentra publicado en el aplicativo SIG en el módulo del SGSI.

MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN

El Ministerio de Educación Nacional cuenta con el Plan del Sistema de Seguridad de la Información, lo anterior para dar cumplimento a las directrices de la Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” del Ministerio de Tecnologías de la

Información y las Comunicaciones. Por lo anterior realizó un autodiagnóstico del Modelo de Seguridad y Privacidad de la Información.

Como parte este autodiagnóstico se modificaron y crearon algunos documentos que hacen parte del proceso de Gestión de Servicios TIC:

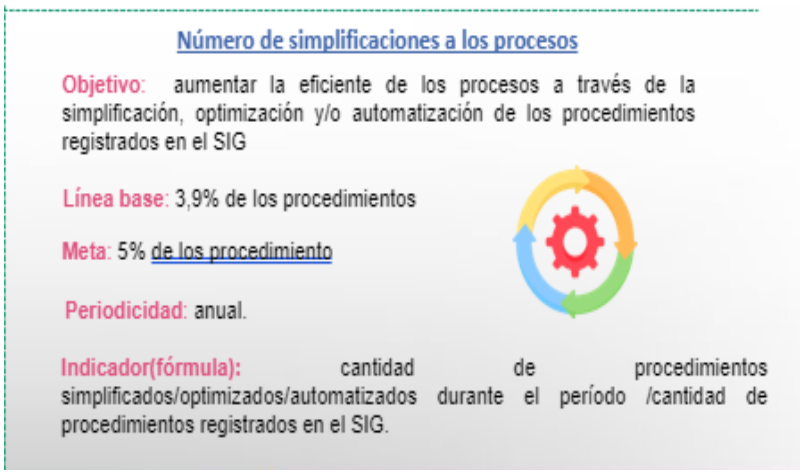
Creados:

• Guía de política de control de acceso ST-GU-19_V1
• Procedimiento – Gestión de incidentes de seguridad de la información ST-PR-18_V1
• Guía de política de seguridad en la nube ST-GU-20_V1
• BIA: Análisis de impacto del negocio
• DPR: Plan de recuperación de desastres
• Guía de Hardening para los sistemas de información (Fortalecimiento a los sistemas de información)

Modificado:

Manual de política de seguridad ST-MA-05_V2

Revisando el índice de mejora propuesto por la Subdirección de Desarrollo Organizacional en la reunión de enlaces de 2022, donde se solicita a las dependencias del Ministerio realizar optimización de documentos oficializados en el SIG (anexos, formatos, guías, instructivos manuales, procedimientos entre otros), como se presenta en el siguiente gráfico:



Fuente: Reunión-Enlaces Subdirección de Desarrollo Organizacional

Se observó en la relación de documentos de servicios TIC publicados en el SIG la siguiente información:

Documentos publicados en el SIG con corte a octubre 2022Documentos	Cantidad
ANEXO	13
CARACTERIZACIÓN	1
FORMATO	25

Etiquetas de fila	2019	2020	2021	2022	Total general
ANEXO			8	5	13
CARACTERIZACIÓN				1	1
FORMATO	11	4	6	4	25

GUÍA	22	GUÍA		16	3	3	22
INSTRUCTIVO	4	INSTRUCTIVO	3			1	4
MANUAL	5	MANUAL	2	2		1	5
PLAN	2	PLAN				2	2
PROCEDIMIENTO	19	PROCEDIMIENTO	3	2	8	6	19
PROTOCOLO	1	PROTOCOLO	1				1
Total general	**92**	**Total general**	**20**	**24**	**25**	**23**	**92**

Fuente: Reporte Documentos Oficializados SIG-OTSI

En el cuadro anterior se puede observar documentos con antigüedad de 4 años sin modificación y/o actualización, como, por ejemplo:

DOCUMENTO	FECHA ULTIMA ACTUALIZACIÓN
Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas ST-PT-01 V3	13 DE NOVIEMBRE DE 2018
Procedimiento Gestión Catálogo de Servicios y Niveles de Servicio ST-PR-01 V3	11 DE NOVIEMBRE DE 2018
Instructivo Modelo de Operación Código: ST-IN-02 V3	13 DE NOVIEMBRE DE 2018
Manual de Políticas de Servicios TIC Código: ST-MA-03	6 DE DICIEMBRE DE 2018
Instructivo Lineamientos Gestión de Cambios	13 DE NOVIEMBRE DE 2018

Fuente: Reporte Documentos Oficializados SIG-OTSI

Así las cosas, se recomienda a la dependencia analizar si se requiere la actualización ajuste y/o eliminación de los documentos que presentan más de dos años sin modificaciones, tal como le señala en el PROCEDIMIENTO DE CONTROL DE DOCUMENTOS DEL SIG PM-PR-01 versión 7. Es importante, tener en cuenta que la operación de la entidad se soporta en la gestión por procesos, la cual es dinámica y se ajusta a las necesidades de esta y a los cambios del entorno.

PARTICIPACIÓN 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.

RESUMEN EJECUTIVO

CONCLUSIONES	RECOMENDACIONES
PROCEDIMIENTO GESTIÓN DE ACTIVOS DE INFORMACIÓN ST-PR-16 V.01 La actividad "Determinar viabilidad de la actualización de los activos de información" no se está realizando con el Coordinador del Grupo de Gestión Documental (Unidad de Atención al Ciudadano).	Validar las actividades del procedimiento Gestión de Activos de Información de tal forma que se realice de conformidad a lo establecido.
GUÍA CLASIFICACIÓN DE LA INFORMACIÓN ST-GU-17 V. 01. En la Guía clasificación de la Información ST-GU-17 en su versión 1, de acuerdo con la normatividad vigente, el MEN definió los roles relacionados con la gestión de activos de información de la siguiente manera: - Responsable de la producción de información Productor. - Responsable o custodio de la Información, encargado del control - Custodio. - Técnico. - Responsable de seguridad de la información – Seguridad - Jurídico. - Gobierno Digital. - Aprobador. Al realizar la validación del rol del jurídico a través de la Oficina Jurídica, no se evidenció que se haya tenido acompañamiento de concepto u orientaciones sobre los datos que son susceptibles de poner a disposición de cualquier individuo, tal como se establece en la Guía.	Validar las actividades de la Guía clasificación de la Información ST-GU-17 de tal forma que se realice de conformidad a lo establecido.
RIESGOS Y EVALUACIÓN DE CONTROLES En la validación de riesgos se pudo determinar lo siguiente: - Las actividades de los controles, capacitaciones se programaron a julio dado que para esa fecha estaba la operación. (No reportan los adjuntos, lista de asistencia y presentación). - El control identificado en el riesgo evaluado "lideres de línea realiza seguimiento a los Bug" presenta un informe con corte a junio de 2021 que no corresponde al periodo evaluado por la dependencia.	Validar la estructura de los controles y su diseño, así como el medio de verificación de estos, para facilitar la evaluación de la eficacia de los mismos Por otro lado, revisar la adecuada formulación de las actividades relacionadas con el plan de manejo, de tal forma que estas no sean las mismas asociadas al medio de verificación del control.

CONCLUSIONES	RECOMENDACIONES
- En el caso del control “El líder valida trimestral los RFC” la Oficina de Control Interno sugiere verificar la periodicidad, ya que no se identificó evidencia de toma de conciencia, informe, ni actas. - Para el control “El líder valida el resultado de vulnerabilidades” se recomienda validar si se va a presentar un informe o el medio de verificación a registrar en el SIG. - En el caso de los riesgos nivel extremo que se identificaron que las actividades de Control son las mismas formuladas para el plan de manejo.	
ACTIVOS DE INFORMACIÓN Se validaron los activos de información del proceso de Gestión de Servicios TIC, quienes tienen identificados los riesgos de seguridad digital para 5 de los 6 activos con valor Alto, clasificados como Información Pública Reservada.	Validar los activos de información del proceso de tal forma que se identifiquen dentro los riesgos de Seguridad Digital.
MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN En la validación de documentos oficializados en el aplicativo SIG, se observaron algunos con antigüedad de 4 años sin modificación y/o actualización.	Analizar si se requiere la actualización ajuste y/o eliminación de los documentos que presentan más de dos años sin modificaciones, tal como le señala en el PROCEDIMIENTO DE CONTROL DE DOCUMENTOS DEL SIG PM-PR-01 versión 7. Es importante, tener en cuenta que la operación de la entidad se soporta en la gestión por procesos, la cual es dinámica y se ajusta a las necesidades de esta y a los cambios del entorno.

INFORME DETALLADO

Resultado		Descripción	Recomendación
HZ	OM		
		No se determinaron para la presente auditoria.	

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES

Resultado			Requisito o Numeral	Descripción
C	NC	OM		
			No aplica	

LÍDER DEL EQUIPO AUDITOR: MONICA GONZALEZ MORENO

JEFE OFICINA DE CONTROL INTERNO: MARIA HELENA ORDOÑEZ BURBANO