ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

SECRETARÍA DE EDUCACIÓN DEL DISTRITO

INFORME DE SEGUIMIENTO SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

31 de octubre de 2024

Av. El Dorado No. 66 - 63
PBX: 324 1000 - Fax: 315 34 48
Código postal: 111321
www.educacionbogota.edu.co

BOGOTÁ

TABLA DE CONTENIDO

1. OBJETIVO.

Verificar la implementación de controles establecidos en el mapa de riesgos de seguridad digital 2024 y la Política de Seguridad Digital de la dimensión 3 "Gestión con valores para resultados" del Modelo Integrado de Planeación y Gestión - MIPG.

1.1 Objetivos específicos

- Evaluar el nivel de cumplimiento de los planes de mejoramiento de seguridad y privacidad de la información de la Secretaría de Educación del Distrito implementados durante los años 2022 y 2023.
- Verificar el cumplimiento de la Norma Técnica de Calidad NTC-ISO/IEC 27001 y la Resolución 500 de 2021, disposiciones que establecen los estándares para la correcta implementación del Sistema de Gestión de la Seguridad de la Información velando por la confidencialidad, integridad y disponibilidad de esta mediante la aplicación de un proceso de gestión del riesgo.
- Evaluar los resultados de gestión de las políticas 7 y 8 del MIPG, "Gobierno y Seguridad Digital", en el marco de la medición del índice de desempeño institucional que realiza el DAFP a través del Formulario Único de Reporte y Avance de Gestión FURAG.

2. ALCANCE.

Comprende la revisión de gestión adelantada por la Oficina de Tecnologías de la Información y las Comunicaciones como dependencia líder en la implementación del modelo de seguridad y privacidad de la información y de la política de seguridad digital.

El periodo de seguimiento comprendió del 16 de septiembre de 2023 al 01 de septiembre de 2024, adicionalmente se contempla la descripción y evidencias de ejecución de actividades con ocasión de las recomendaciones incluidas en el cuerpo del informe de seguimiento realizado por la Oficina de control Interno mediante oficio I-2022-115761 del 31 de octubre de 2022 y I-2023-141350 del 13 de diciembre de 2023.

El alcance de esta evaluación incluyó:

1. **Revisión de Documentación**: Análisis de los documentos relacionados con los planes de mejoramiento, incluyendo políticas, procedimientos, y registros de actividades realizadas durante los años 2022 y 2023.
2. **Evaluación de Implementación**: Verificación de la implementación efectiva de las acciones correctivas y preventivas propuestas en los planes de mejoramiento, asegurando que se hayan llevado a cabo de acuerdo con los cronogramas establecidos.
3. **Cumplimiento Normativo**: Evaluación de la conformidad con los requisitos de la NTC-ISO/IEC 27001 y la Resolución 500 de 2021, asegurando que las prácticas de gestión de la seguridad y privacidad de la información cumplan con los estándares y regulaciones vigentes.
4. **Revisión resultados FURAG**: Revisión y análisis de la medición a la gestión de las políticas 7 y 8 del MIPG, identificando áreas, actividades o elementos de política con menores índices.
5. **Análisis de Resultados**: Comparación de los resultados obtenidos con los objetivos establecidos en los planes de mejoramiento y las normativas aplicables, identificando áreas de éxito y oportunidades de mejora.

6. **Recomendaciones**: Propuesta de recomendaciones específicas para fortalecer la gestión de la seguridad y privacidad de la información, basadas en los hallazgos del seguimiento y la evaluación normativa.

3. CRITERIOS

Los criterios del presente seguimiento son:

3.1 Cumplimiento Normativo:

- Constitución política de Colombia
- Ley 87 de 1993 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones”.
- Ley 594 de 2000 “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 305 de 2008 Secretaría General Alcaldía Mayor de Bogotá D.C., “Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre”.
- Resolución 004 de 2017 Secretaría General Alcaldía Mayor de Bogotá D.C., por la cual se modifica la Resolución 305 de 2008 de la Comisión Distrital de Sistemas.
- Resolución 1944 de 2017 “Por medio de la cual se adopta la Política de Seguridad de la Información de la Secretaría de Educación de Distrito”.
- 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".
- Resolución 746 de 2022,” Por la cual se fortalece el modelo de seguridad y privacidad y se definen lineamientos adicionales a los establecidos en la resolución 500 de 2021”.
- Acuerdo 927 de 2024 Por medio del cual se adopta el Plan de Desarrollo Distrital 2024-2027 "Bogotá Camina Segura".
- Directiva 5 de 2005 de la Alcaldía Mayor, Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital.
- Directiva 08 de 2021, Alcaldía Mayor de Bogotá. “Lineamientos para prevenir conductas irregulares con el incumplimiento de los manuales de funciones y competencias laborales y de los manuales de procedimientos institucionales, así como por la pérdida, o deterioro, o alteración o uso indebido de bienes, elementos, documentos públicos e información contenida en bases de datos y sistemas de información”

Otros

- Conpes 3701 de 2011 lineamientos de políticas para ciberseguridad y ciberdefensa.
- Conpes 3854 de 2016 Política nacional de seguridad digital.
- Conpes 3995 de 2020, Política nacional de confianza y seguridad Digital.

- Norma Técnica Colombiana NTC – ISO/IEC 27001 -2013.
- Manual Operativo del Modelo Integrado de Planeación y Gestión V.5
- Política de Gobierno Digital –Componente Seguridad y Privacidad de la Información.
- 12-MG 01 Metodología de Administración para la gestión de los Riesgos de Seguridad Digital.
- Plan de acción Modelo de Seguridad y Privacidad de la Información 2023.
- Mapas de riesgos del proceso Gobierno y Seguridad Digital, de corrupción 2023.
- Plan Estratégico de Tecnologías de la Información 2020-2024.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas.
- Matriz gestión de riesgos de seguridad digital.

4. RESULTADOS.

Para el informe de seguimiento, se utilizaron las siguientes siglas:

- CIGD Comité Institucional de Gestión y Desempeño
- SED Secretaría de Educación del Distrito
- OCI Oficina de Control Interno
- OTIC Oficina de Tecnología de la Información y las Comunicaciones
- OAP Oficina Asesora de Planeación
- MSPI Modelo de Seguridad y Privacidad de la Información
- TI Tecnologías de la Información
- TIC Tecnologías de la Información y las Comunicaciones
- MECI Modelo Estándar de Control Interno
- MIPG Modelo Integrado de Planeación y Gestión
- PSPI Plan de Seguridad y Privacidad de la Información
- MAGRSD Metodología de Administración para la Gestión de los Riesgos de Seguridad Digital
- PETIC Plan Estratégico de Tecnologías de Información y Comunicaciones
- SGSI Sistema de Gestión de Seguridad de la Información.
- CIGD Comité Institucional de Gestión y Desempeño institucional
- CSIRT Equipo de Respuesta a Incidentes de Seguridad Digital
- MINTIC Ministerio de las Tecnologías y Comunicaciones

4.1 Evaluación recomendaciones pendientes informe de seguimiento del año 2022 y de la Auditoría 2023.

Con base en la solicitud enviada a la OTIC, radicado I-2024-105212 con asunto: Seguimiento Seguridad Digital y Seguridad de la Información 2024 del 10 de septiembre de 2024 y frente al cual la OTIC remitió radicado de respuesta I-2024-113445 del 27 de septiembre de 2024 y cargó parte de la evidencia en el repositorio de share point dispuesto para tal fin, se pudo observar que, en cuanto al avance en el cumplimiento de las recomendaciones del seguimiento del 2022 y de la auditoría del 2023 se encontraron distribuidas así:

Gráfico 1. Cumplimiento de recomendaciones del 2022 y 2023.

Fuente: Elaboración equipo auditor – Evidencia presentada por la OTIC

Recomendaciones seguimiento 2022 y Auditoria 2023			
CUMPLIDAS	2022	Construcción Metodología de Administración para la Gestión de los Riesgos de Seguridad Digital	
	2022	Fortalecimiento y aplicación Metodología de Administración para la Gestión de los Riesgos de Seguridad Digital	
	2023	Herramienta de seguimiento a proyectos de la OTIC	
	2023	Diagnostico MSPI	
PARCIALMENTE CUMPLIDAS	2023	Politica de seguridad digital	
	2023	Plan de continuidad de negocio	
INCUMPLIDAS	2023	Hallazgos abiertos años anteriores sin porcentaje de avance	

Fuente: Elaboración equipo auditor – Evidencia presentada por la OTIC

Frente a las dos recomendaciones pendientes de cumplimiento del seguimiento del 2022 se pudo evidenciar que se cumplieron. Así mismo, se pudo establecer que la MAGRSD vigente está en proceso de actualización por lo que se recomienda culminarla y publicarla para conocimiento de la SED, adicionalmente la OTIC ha remitido evidencia de la aplicación de controles y disposiciones contenidas en dicha metodología con el fin de salvaguardar la el manejo de la información y de control sobre los diferentes equipos en el data center y cuartos de comunicaciones y diferentes equipos conexos, a fin de dar continuidad de las operaciones de la entidad. Así mismo, ha realizado el acompañamiento a las diferentes áreas para la Construcción de la matriz de riesgos de seguridad digital, matriz de riesgos que ya se puede consultar en el Power BI en Isolución.

En cuanto a las cinco recomendaciones pendientes de la Auditoría del 2023, dos se encontraron cumplidas, dos con cumplimiento parcial y una no cumplida. De las cumplidas, se puede resaltar los avances en la construcción de la herramienta de seguimiento de proyectos de Sistemas de

Información actualizada a 2024, la cual se conformó de acuerdo con las necesidades de seguimiento de los proyectos, con el fin de obtener información del avance en cada una de las etapas y de conocer el estado de cada proyecto. La otra recomendación cumplida fue el levantamiento de un autodiagnóstico del MSPI de la entidad. Las recomendaciones de cumplimiento parcial y no cumplimiento se describen a continuación:

En la verificación efectuada por la OCI respecto a la recomendación enmarcada en la auditoria de Seguridad Digital 2023, "Construcción de una política de seguridad digital para la entidad" se observó que dentro de la evidencia suministrada se encontró el Manual para la prestación de los servicios de tecnologías de la información y las comunicaciones (TIC) publicado en Isolución en el mes de septiembre de 2024, manual que indica que" *...este manual agrupa las políticas individuales aplicables al proceso de Gobierno y Seguridad Digital que hasta la fecha se han definido y a las que a futuro puedan establecerse en observancia de la normatividad vigente...",* evidencia que no corresponde con el documento esperado, incumpliendo parcialmente el criterio contenido en la Resolución 500 de 2021 del MINTIC, que establece: *"ARTÍCULO 5. La estrategia de seguridad digital. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital.(..) la estrategia debe ser aprobada a través de un acto administrativo de carácter general (…) y La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.";* desconociendo además los lineamientos para el MSPI impartidos por MINTIC "Documento Maestro del Modelo de Seguridad y Privacidad de la Información de MINTIC", que establecen que: "*Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño*".

Lo anterior, debido a un posible desconocimiento de la norma y de los instrumentos de orientación impartidos por MINTIC teniendo como consecuencia posibles sanciones por incumplimiento normativo. No obstante el presente seguimiento considera la recomendación con cumplimiento parcial, ya que existe la "política de seguridad de la información" para la entidad, resolución 1944 de 2016 que contiene disposiciones generales orientadas a preservar la confidencialidad de los activos de información, y si bien esta no contempla el concepto de seguridad digital y la protección de toda la infraestructura, sistemas, redes y dispositivos informáticos de la entidad, es un avance encaminado al cumplimiento del criterio señalado.

Dado lo anterior, se eleva una alerta a la OTIC y se recomienda consolidar la política de gobierno digital que integre la estrategia de seguridad digital de la entidad así como asegurar que las políticas relacionadas con el MSPI que se encuentran publicadas en el portal web de la entidad sean, en primera instancia, avaladas por el Comité Institucional de Gestión y Desempeño, y respaldadas mediante acto administrativo que manifieste la voluntad de la alta dirección, ya que afectan el funcionamiento interno de la entidad y se debe procurar su apropiación por parte de funcionarios y contratistas.

Otra recomendación de la auditoria 2023 con cumplimiento parcial, corresponde al fortalecimiento de los mecanismos en el proceso de definición e implementación del plan de continuidad de negocio, ya que se encontró que se ha construido documentación que permita establecer las acciones y estrategias a seguir ante los diferentes riesgos a los que se expone la SED y poder tener un plan de continuidad del negocio; se allegó un documento denominado "Plan Continuidad V13", cuyo objetivo es: *"definir las actividades a seguir antes, durante y después de la ocurrencia de un evento tipo desastre para garantizar la recuperación, continuidad de los sistemas de información y la prestación del servicio de TIC de la Secretaría de Educación de Distrito, reestableciendo los procesos críticos*

de forma óptima, minimizando los tiempos de indisponibilidad", documento que no se encuentra formalizado ni publicado en la SED.

Alerta 1: Hallazgos sin avance años anteriores ⚠

La recomendación incumplida corresponde a los hallazgos del 2023, de los cuales se lograron cerrar dos y aparecen tres de ellos aún abiertos, 1567,1569 y 1570 con un avance del 0% según se reporta en Isolución, por lo que las evidencias de gestión para subsanar dichos hallazgos allegadas a este seguimiento es necesario que se carguen en el aplicativo, cuyo proceso de valoración se hará al final del mes de octubre por parte de la OCI. A su vez se estableció que a la fecha del seguimiento se observan en total 14 hallazgos abiertos para la OTIC en el aplicativo por lo que se reitera la necesidad de gestionar las evidencias para subsanarlos.

4.2. Avance en acciones descritas en el Anexo No 1. PSPI 2023

Referente a dicho avance sobre las diecisiete recomendaciones que se indicaron en la solicitud a la OTIC, que fueron catalogadas con cumplimiento parcial o no cumplimiento en el PSPI de la vigencia 2023, la OTIC, cargó evidencia parcial de lo logrado en el 2023 y suministró evidencia de algunas recomendaciones adelantadas en 2024, por lo que se optó por valorar de acuerdo a lo evidenciado independientemente del año, siendo así que del ejercicio se concluye que del total de acciones se ha logrado cumplir con el 65% (doce acciones), con cumplimiento parcial en el 24% de ellas (cinco acciones) y 12% en acciones no cumplidas (dos acciones), avance que se puede observar a continuación:

Gráfico 2. Cumplimiento de Acciones del Anexo 1 PSPI 2023.

Fuente: Elaboración equipo auditor – Evidencia presentada por la OTIC

Del ejercicio, se puede observar avances en el tema del Plan de Continuidad del negocio, en donde se esboza la construcción del plan, el cual está pendiente de publicación; a su vez se pudo ver que ya es posible el apostillaje o legalización de los documentos certificados por la Secretaría de

Educación de Bogotá vía web en la Cancillería. El estado de cada una de las acciones se indica en el anexo 1 de este informe.

Imagen 1. Evidencia apostillaje vía web.

Fuente: https://tramites.cancilleria.gov.co/apostillalegalizacion/solicitud/inicio.aspx

Alerta 2: Avance proyecto EGD-POA-SISAE ⚠

En cuanto a la recomendación de la auditoria, referente a la consolidación de una herramienta para el Seguimiento de los proyectos de TI de la OTIC, se pudo observar que en promedio se tiene un porcentaje real de avance en los 14 proyectos del 74%, proyectos que se deben culminar en esta vigencia según la evidencia suministrada, sin embargo se encuentra un proyecto con bajo avance en su ejecución, como lo es el de EGD-POA-SISAE (24%), cuya entrega está programada para culminarse en el mes de octubre de 2024.

Una acción con cumplimiento parcial es la "Estrategia de Uso y apropiación TIC de la entidad", si bien la OTIC remitió plan de capacitación incluyendo charlas y talleres sobre big data, innovación y software en específico, no se suministró información sobre la realización y resultados de capacitaciones en seguridad informática, adicionalmente según el propio concepto de la OTIC la etapa de divulgación de la estrategia TIC se encuentra aún en consolidación.

Una de las actividades propuestas en el PSPI 2023 fue "definir un modelo de gobierno de TI", para esta actividad la evidencia esperada era la "construcción de una política de gobierno digital para la entidad", no obstante, la evidencia que se remitió formalizó y divulgó, fue el "manual de servicios de TI", que se mencionó anteriormente, aprobado el 23 de septiembre de 2024. Dicho manual fue avalado por la OAP de acuerdo con la información remitida por la OTIC, considerándose así que el manual "agrupa las políticas asociadas". Ahora bien, teniendo en cuenta el análisis realizado en el punto 4.1 del presente seguimiento el Manual mencionado, no cumple con los requerimientos de la norma.

En otro sentido, se evidencia un cumplimiento parcial de la recomendación "Actualizar las políticas asociadas al MSPI y socializarlas". Aunque la OTIC publicó en la web de la entidad la "política de datos personales", la "política de privacidad y condiciones de uso de portales web", la "política de uso y manejo del correo electrónico" y la "política de privacidad y seguridad de la información", solo esta última fue debidamente formalizada mediante el acto administrativo, Resolución 1944 de 2016, política que no incluye disposiciones a propósito de toda la infraestructura digital (sistemas, redes y dispositivos) de la entidad como se mencionó anteriormente.

Adicionalmente, los otros instrumentos orientativos han sido aprobados por la OTIC y se encuentran publicados en la página web de la entidad, más no han sido formalizados a través de un acto administrativo, lo que desconoce los lineamientos para el MSPI impartidos por MINTIC "Documento Maestro del Modelo de Seguridad y Privacidad de la Información de MINTIC" que establece: "*Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño*".

Por lo demás, la OTIC evidencia el plan de tratamiento de riesgos de seguridad informática con la debida identificación de activos, refiere y adjunta la existencia de un autodiagnóstico del MSPI para la entidad y presenta informe de seguridad en los servicios publicados en los dominios .edu y .gov; acciones enmarcadas en el PSPI vigencia 2023 que se cumplieron a cabalidad.

Alerta 3: Información incompleta requerimientos OCI ⚠

Se pudo establecer que, para las siguientes recomendaciones contempladas en el PSPI 2023, no se cargó evidencia de ejecución, por ende, su valoración se consideró incumplida:

- Seguimiento al contrato de implementación de protocolo IPV6.
- Campaña de sensibilización para directivos, funcionarios y usuarios sobre IPV6 y la transición realizada en la entidad.

Al respecto es importante mencionar que la OCI remitió cuestionario a través de radicado I-2024-105212 a la OTIC , con el objetivo de obtener evidencia de la ejecución de las actividades mencionadas específicamente en la pregunta 7 numeral 17, de dicho cuestionario, obteniendo como respuesta de la OTIC: " Se realiza el cargue correspondiente a la transferencia de conocimiento a los usuarios de la SED, Planillas de Asistencia Grabaciones de las sesiones Presentación"; sin embargo los documentos mencionados no se encuentran para consulta en el espacio "share point" dispuesto para tal fin. Lo anterior, generando como consecuencia que esta dependencia no obtenga información real sobre la ejecución de las actividades y desconociendo el deber de entrega, oportunidad y coherencia de información.

Adicionalmente, en marco del seguimiento se realizó consulta a través del SECOP del contrato de implementación IPV6 SED-LP-REDP-008-2022 evidenciando que para el mismo no existe informe de ejecución ni interventoría.

4.3 Cumplimiento de la NTC NTC-ISO/IEC 27001- 2013:

La Norma Técnica de Calidad NTC-ISO/IEC 27001-2013 establece los requisitos para implementar, mantener y mejorar continuamente un SGSI; esta orientación, establece dimensiones imprescindibles para lograr una adecuada implementación del sistema como lo son la identificación del contexto de la organización, el liderazgo, la planificación, el soporte, la adecuada operación, la evaluación y el tratamiento de no conformidades y acciones correctivas. Cada una de las dimensiones se desarrolla en la existencia de controles que fueron evaluados para la entidad y los resultados relevantes se presentan a continuación.

De la evaluación realizada, se encontró inicialmente que la OTIC ha elaborado un autodiagnóstico sobre el estado de implementación del MSPI en atención a las disposiciones normativas y a las orientaciones de MINTIC, dicho diagnostico ubica a la entidad en un **nivel inicial** de madurez en la

implementación de estrategias de seguridad. Este nivel se debe principalmente a la falta de reporte y evidencias de gestión de incidentes de seguridad. Además, se identificó que no se realiza plan de mejoramiento para los incidentes identificados, disposición que es obligatoria según la NTC.

Si bien se reconoce que la entidad cuenta con políticas relacionadas con el MSPI como se ha venido mencionando y que estas se encuentran publicadas en la página web de la entidad junto con el Manual de la Política General de Gestión de Seguridad de la Información, se evidencia que no todas las políticas publicadas fueron constituidas con actos administrativos y que no han sido aprobadas por el CIGD, como se indicó en el numeral 4.1 del presente informe de seguimiento. Por lo que se recomienda **definir y divulgar una jerarquía documental** de la estrategia de seguridad digital.

Ahora bien, en lo referente al control "organización de la gestión de SI", como se ha reconocido, la SED formalizó el Manual de la Política General de Gestión de Seguridad de la Información. No obstante, este instrumento no aborda un subcapítulo relativo a la seguridad de la información en el contexto de trabajo remoto y para dispositivos móviles.

En lo referente al control de recursos humanos, numeral 7 de la norma, se encuentra que el plan de capacitación presentado por la OTIC como respuesta al formulario remitido en este seguimiento, no evidencia la realización y resultados de talleres específicamente sobre seguridad informática, uso adecuado de la red institucional, manejo del correo electrónico u otros temas relacionados durante 2024. Tampoco se refieren los resultados de capacitaciones relacionadas en 2023.Si bien en el referido plan la OTIC advierte que se tienen programadas charlas al respecto, "talleres de seguridad" y "socialización de la política de gobierno digital" para 2023, no hay evidencias sobre la realización de estas e incluso a la fecha es inexistente la política de gobierno digital.

Respecto al control y gestión de incidentes, numeral 12 de la norma, la OTIC menciona la construcción de un acervo documental para la gestión de incidentes (caracterización de procedimientos), pero no documenta los incidentes ni los reporta a través de planes de mejoramiento o instrumentos para corregir lo actuado, aspecto que como se mencionó resalta la debilidad del MSPI. Aspecto que se desarrollará más adelante en observancia del criterio dispuesto por la Resolución 500 de 2021.

En cuanto al control referente a las comunicaciones, numeral 13 de la norma, que recomienda acciones diseñadas para proteger la confidencialidad e integridad de la información que se transmite por medios magnéticos o digitales; se evidencia la existencia de un acuerdo de confidencialidad genérico que solo se aplica a los proyectos desarrollados en la entidad a libre discreción, bajo las consideraciones del presente seguimiento, la acción es insuficiente, pues aunque la información manejada por la Secretaría de Educación Distrital es en su mayoría de carácter público, parte de ella puede estar sujeta a acuerdos de confidencialidad y no divulgación, especialmente tratándose de datos sensibles de menores de edad. Por lo tanto, se recomienda identificar información sensible y específica para implementar acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información, en consonancia con la protección de los derechos humanos y caracterizando información sensible.

Por otra parte, en atención a lo dispuesto por el artículo 2.2.22.3.14 del Decreto 1083 del 2015 "Único Reglamentario del Sector Función Pública" , las entidades públicas deben integrar al plan de acción, en consonancia con el MIPG , el plan de tratamiento de riesgos de seguridad y privacidad de la información, en consecuencia, la OTIC ha construido el plan referido, presentando evidencias de seguimiento, aplicación de controles y análisis de gestión del riesgo asociados a la seguridad informática, dicha evidencia se encuentra publicada en la página web de la entidad.

El instrumento desarrollado por la OTIC considera riesgos asociados a la vulnerabilidad de la seguridad informática de la entidad (como robo de información sensible, filtración de datos o interrupción de servicios) y la posibilidad de impacto en la prestación de servicios tecnológicos por el inadecuado uso de los servicios informáticos o por otras causas derivadas de la inmadurez del MSPI.

Lo anterior, en cumplimiento del tercer componente del MECI, cuyo objetivo es fortalecer la identificación, evaluación y gestión de aquellos eventos, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos institucionales.

Finalmente se encuentra, que la Secretaría de Educación del Distrito a través de la OTIC establece, documenta, implementa y mantiene los procesos, procedimientos y controles para los planes de continuidad, y determina sus requisitos para la seguridad de la información en situaciones adversas (crisis o desastres), más no ha culminado la construcción del Plan de Continuidad del Negocio. Sin embargo, aunque se evidencia que existe una programación de actividades para el año 2024, en relación con el Plan de Acción Anual para la implementación y seguimiento del MIPG, es necesario monitorear el avance de actividades ya que se evidencia un 0% de avance, de acuerdo con lo evidenciado en la respuesta a la pregunta 2 del cuestionario que soporta este informe, esto posiblemente en razón a la falta de seguimiento y digitalización de la herramienta.

4.4 Cumplimiento de la Resolución 500 de 2021:

La Resolución 500 de 2021 del MINTIC, expone que las entidades públicas deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI.

Observación 1: Control de incidentes

La SED cuenta con una estrategia de seguridad digital aunque no la ha formalizado en acto administrativo de carácter general (punto 4.1 de este seguimiento) y aplica controles para mitigar los riesgos derivados de fallas en los sistemas informáticos, no obstante, como se mencionó anteriormente, falla en el reporte de la gestión de incidentes, pues en la verificación efectuada por este despacho respecto al reporte de incidentes informáticos a la Alta Dirección se evidenció que en las actas del Comité Institucional de Gestión y Desempeño de 2019 a la fecha, no se abordó reporte de incidentes o informe de gestión de los mismos, en omisión de la resolución 500, el artículo 6, numeral 3: "*Responsabilidades de los sujetos obligados: Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces";* generando la posibilidad de materializar sanciones para la entidad.

Observación 2: Plan de capacitación en seguridad informática

Se identificó adicionalmente que la OTIC no suministró evidencia respecto a lo estipulado en el artículo 6, numeral 5 de la Resolución, este numeral instaura la siguiente responsabilidad: *"Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas".* Al respecto, se evidencia, falta de alineación con las directrices establecidas en dicha normatividad, así como falta de documentación, ya que no se allegaron registros que respalden el cumplimiento del requisito mencionado durante el plan de capacitaciones 2023, lo anterior desarrollado en el punto 4.3 del presente seguimiento, generando la posibilidad de materializar sanciones para la entidad.

4.5 Seguimiento a los resultados del índice de desempeño institucional para las políticas 7 y 8 MIPG.

Teniendo en cuenta que los resultados de la medición del desempeño institucional 2023, que mide anualmente la gestión y desempeño de las entidades públicas, proporcionando información para la toma de decisiones en materia de gestión y control interno, podemos observar el comportamiento de la entidad en el MIPG, cuyos resultados de la vigencia 2023 son comparables con los resultados de la medición de la vigencia 2022, podemos observar que la SED tuvo una ligera caída en los resultados del 2023.

Tabla 4. Resultados FURAG en Política MIPG 2022-2023

POLÍTICA MIPG	FURAG 2022	FURAG 2023
Gobierno Digital	85	84,8
Seguridad Digital	88,6	87,1

Fuente: Elaboración equipo auditor – Consulta en Función Publica

Consultando el Power BI de Función Pública, se esboza los resultados generales en cuanto a la Política 7 de Gobierno Digital para la vigencia 2023, en donde se identifica que la entidad ha obtenido una calificación del 84.8% como se puede observar en la imagen 1. Ahora, analizando los resultados de los once subíndices que la conforman se dejan a continuación las recomendaciones que destaca el reporte, que la entidad requiere para mejorar su calificación en esta política como son:

1. *Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y tomar las medidas necesarias para evitar que se vuelvan a presentar.*
2. *Aprobar y publicar la licencia de datos abiertos de la entidad, mediante la cual se determina el alcance, uso y aprovechamiento que los particulares o terceros interesados puedan efectuar sobre los mismos.*
3. *Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).*
4. *Capacitar a servidores y contratistas de la entidad en la Política de Gobierno Digital implementando estrategias como los cursos dispuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones; las capacitaciones dispuestas en el Plan de Capacitaciones de la entidad; entre otras.*
5. *Contar con un proceso para la gestión de datos maestros en la entidad.*
6. *Contar con una plataforma para la gestión y distribución de datos maestros en la entidad.*
7. *Desarrollar conjuntos de datos abiertos estratégicos de la entidad en procesos de cocreación o consulta pública.*
8. *Digitalizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).*
9. *Disponer todos los documentos resultantes de los trámites de la entidad en la Carpeta Ciudadana Digital.*
10. *Implementar estrategias de mejora de los trámites parcialmente en línea de la entidad para aumentar el número de usuarios satisfechos con su uso.*
11. *Integrar el proceso de gestión de proyectos con componentes de TI con el Sistema de Gestión de Calidad de la entidad.*
12. *Realizar auditorías internas, externas y de certificación o recertificación respecto al estándar ISO 27001 en la entidad.*
13. *Realizar pruebas de recuperación de cada uno de los sistemas de información críticos*

14. Usar el servicio de Carpeta Ciudadana Digital para que la entidad reduzca el número de PQRSD, reduzca los tiempos de respuesta de los trámites, reduzca el consumo de papel necesario para dar respuesta a los trámites, entre otros.
15. Utilizar medios digitales como redes sociales o la sede electrónica de la entidad para los ejercicios de rendición de cuentas.

Por otra parte, en el informe de empalme del año 2023 de la SED en el numeral 2.3.2 Gobierno Digital en la Tabla 19 Avance Habilitadores Gobierno Digital, se estipulan los retos que la SED tiene en materia de esta política, por lo cual se exhorta a la SED en tener en cuenta, tanto estos, como las recomendaciones relacionadas anteriormente producto de los resultados de la Medición del Desempeño Institucional 2023 en el FURAG.

Imagen 1. Resultados FURAG en Política de Gobierno Digital

Fuente: https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

Se evidencia un puntaje de 84.8 % en el reporte del FURAG del 2023, menor a lo esperado en la dimensión de la política de gobierno digital "decisiones basadas en datos", esto como consecuencia de que si bien, la entidad cuenta con un inventario y diccionario de datos para el sistema de información de POA, no refiere documentar e implementar un modelo de gobierno de datos que defina cómo se gestionan, protegen y utilizan los datos dentro de la entidad, tampoco se evalúan las capacidades con relación al uso y explotación de datos. De acuerdo con las respuestas al cuestionario FURAG, la entidad no refiere haber levantado un catálogo para la gestión de datos maestros, ni tenerlos identificados; cuestión que reviste una oportunidad de mejora.

Imagen 2. Resultados FURAG en Política de Gobierno Digital y de Seguridad Digital

Fuente:
https://app.powerbi.com/view?r=eyJrIjoiMzA3NjVjNDctNDVkZC00MWI0LWI0ZTQtZjhhZmY5NTg1Y2NmIiwidCI6IjUwNjQwNTg0LTJhNDAtNDIxNi1hODRiLTIiM2VlMGYzZjZjZiIsImMiOjR9

Por otra parte, en cuanto a la política 8 de Seguridad Digital se puede observar en la imagen 3 que la entidad obtuvo una calificación del 87,1% y se relacionan a continuación las recomendaciones dadas en el reporte de Función Pública en cuanto a los tres subíndices que la componen:

1. Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y tomar las medidas necesarias para evitar que se vuelvan a presentar.
2. Contar con un Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos.
3. Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad digital (Ciberseguridad) que incluya la notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT).
4. Realizar pruebas de recuperación de cada uno de los sistemas de información críticos.

A su vez se pudo establecer que, según lo reportado en el FURAG, la entidad no utilizó el Modelo de Ciudades y Territorios Inteligentes para desarrollar su Estrategia de Ciudades y Territorios Inteligentes, uno de los once subíndices que desarrollan la Política de Seguridad Digital ya que no se enmarca en los propósitos de la entidad.

Imagen 3. Resultados FURAG en Política de Seguridad Digital

Fuente: https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

5. RECOMENDACIONES.

Las recomendaciones esbozadas a continuación son situaciones sobre las que la OCI insta a tomar medidas para evitar o reducir el riesgo, pero no incumplen ningún criterio de auditoría y por lo tanto no requieren plan de mejoramiento, no obstante, aquellas que tienen asociada una alerta presentan mayor riesgo en el cumplimiento de la gestión de la entidad y en el cumplimiento normativo.

- Se recomienda consolidar una Política de Seguridad Digital y Seguridad en la Información de carácter general que integre disposiciones para la protección de toda la infraestructura informática de la entidad con el objetivo de formalizar la estrategia de seguridad digital en cumplimiento del artículo 5 de la Resolución 500 de 2021 y atendiendo las disposiciones del

Documento Maestro del Modelo de Seguridad y Privacidad de la Información de MINTIC. (Alerta 1 de este seguimiento).

- Se exhorta a la OTIC a culminar la actualización de la MAGRSD que está en proceso de actualización y publicarla para conocimiento de la SED.

- Según lo evidenciado en este seguimiento la OTIC mantiene en total 14 hallazgos abiertos por lo que se reitera la necesidad de gestionar las evidencias que permita subsanarlos, más aún, cuando la valoración de estas se hará al final del mes de octubre por parte de la OCI. (Alerta 2 de este seguimiento).

- En cuanto al seguimiento de los proyectos y de las actividades programadas en el plan de acción anual para la implementación y seguimiento del MIPG , se invita a la OTIC a mantener información actualizada del avance en cada una de las etapas y del estado de cada proyecto a fin de monitorear el avance de cada una de ellas a lo largo del tiempo programado, ya que, como por ejemplo, para el contrato de implementación de protocolo IPV6, no se presentó evidencia de ejecución, ni para la campaña de sensibilización para directivos, funcionarios y usuarios sobre IPV6 y la transición realizada en la entidad; en similar sentido se tiene baja ejecución del proyecto EGD-POA-SISAE. (Alerta 3 de este seguimiento).

- Culminar el proceso de construcción del plan de continuidad del negocio.

- Se exhorta a la OTIC a cumplir con el deber de entrega, oportunidad y coherencia de información para los requerimientos realizados en marco de auditorías y seguimientos con el fin de permitir el desarrollo de la actividad de control de la gestión de manera veraz y considerando la información real de la entidad. (Alerta 4 de este seguimiento)

- Se invita a la entidad a acoger las recomendaciones de las Políticas “Gobierno y Seguridad Digital”, expuestas en este informe a fin de mejorar la puntuación obtenida en el FURAG.

- Este seguimiento ha evidenciado la necesidad de publicar y divulgar las políticas asociadas al MSPI, por lo que se recomienda otorgarles a estas el carácter de acto administrativo y que sean aprobadas por el CIGD en atención al artículo 5 de la resolución 500 de 2021 a fin de involucrar a la alta dirección en la estrategia de seguridad informática.

6. OBSERVACIONES.

Las observaciones contenidas en este informe hacen referencia a situaciones relevantes, hallazgos para los cuales la OCI considera necesario hacer seguimiento, definir acciones de mejora y fortalecer los mecanismos de control:

Observación 1: Control de incidentes

La SED cuenta con una estrategia de seguridad digital aunque no la ha formalizado en acto administrativo de carácter general (punto 4.1 de este seguimiento) y aplica controles para mitigar los riesgos derivados de fallas en los sistemas informáticos, no obstante, como se mencionó anteriormente, falla en el reporte de la gestión de incidentes, pues en la verificación efectuada por este despacho respecto al reporte de incidentes informáticos a la Alta Dirección se evidenció que en las actas del Comité Institucional de Gestión y Desempeño de 2019 a la fecha, no se abordó reporte

de incidentes o informe de gestión de los mismos, en omisión de la resolución 500, el artículo 6, numeral 3: "*Responsabilidades de los sujetos obligados: Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces";* generando la posibilidad de materializar sanciones para la entidad.

Respuesta de la OTIC mediante comunicación interna I-2024-128319 del 30 de octubre de 2024.

R/ La OTIC ha solicitado que se incluya en la agenda del próximo Comité, la presentación del reporte de incidentes informáticos, quedando a la espera de la programación de éste, diligenciando y enviando por correo el formato respectivo.

https://educacionbogota-my.sharepoint.com/:x:/g/personal/cbaezb_educacionbogota_gov_co/EZoluFdEWB9InRB24C0vNRsBYQcvp66hEdmXLldZuGLrqQ?e=efb1Dl

Respuesta del equipo auditor

Se mantiene la observación/hallazgo, en consideración a que la explicación no desvirtúa la situación evidenciada por el equipo auditor y la OTIC debe incluir una acción al respecto dentro del plan de mejoramiento.

Observación 2: Plan de capacitación en seguridad informática

Se identificó adicionalmente que la OTIC no suministró evidencia respecto a lo estipulado en el artículo 6, numeral 5 de la Resolución, este numeral instaura la siguiente responsabilidad: *"Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas".* Al respecto, se evidencia, falta de alineación con las directrices establecidas en dicha normatividad, así como falta de documentación, ya que no se allegaron registros que respalden el cumplimiento del requisito mencionado durante el plan de capacitaciones 2023, lo anterior desarrollado en el punto 4.3 del presente seguimiento, generando la posibilidad de materializar sanciones para la entidad.

Respuesta de la OTIC mediante comunicación interna I-2024-128319 del 30 de octubre de 2024.

R/ La OTIC se permite dar alcance a la evidencia presentada, presentando el informe final de capacitaciones del 2023, al cual es posible acceder en el siguiente vínculo:

https://educacionbogota-my.sharepoint.com/:b:/g/personal/hmoyan_educacionbogota_gov_co/EQXDAIRk1PJGpF3jMBlC6KBbI4z365U4W4vcxvz_c61CA?e=dtBczl

que al abrir desde el documento de repuesta nos direcciona a la URL:

https://educacionbogota-my.sharepoint.com/personal/hmoyan_educacionbogota_gov_co/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fhmoyan%5Feducacionbogota%5Fgov%5Fco%2FDocuments%2FArchivos%20de%20chat%20de%20Microsoft%20Teams%2FInforme%20%5FPlan%5FCapacitaciones%5F%20OTIC%5F%202SEM2023%5Ffinal%2Epdf&parent=%2Fpersonal%2Fhmoyan%5Feducacionbogota%5Fgov%5Fco%2FDocuments%2FArchivos%20de%20chat%20de%20Microsoft%20Teams&ga=1

Se evidencian las diferentes capacitaciones hechas por la OTIC, indicadas en el cuadro que indica que:

En resumen, hemos logrado llegar a:

Temática	Asistentes
Uso y apropiación de tecnologías de la información	207
Divulgación de la política de Gobierno y Seguridad Digital	2.387
Seguridad en redes sociales (Estudiantes)	640
Total Personas	3.240
Total Colegios	Cinco (5)

Por lo anterior, se acepta la explicación y se retira la observación.

7. FIRMAS.

Elaborado por:

ÓSCAR MARIANO HAMON VIASUS
Profesional Universitario OCI

INGRID LORENA GUTIÉRREZ BARRERA
Profesional Universitario OCI

Revisado por:

MARÍA DEL PILAR GONZÁLEZ HENAO
Contratista Oficina de Control Interno

Aprobado por:

ÓSCAR ANDRÉS GARCÍA PRIETO
Jefe de Oficina de Control Interno

ANEXO 1. Estado de avance de las acciones descritas en el Anexo No 1. Consolidado revisión acciones Plan de Seguridad y Privacidad de la Información, vigencia 2023.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
1	Definir esquema de gobierno de T.I (políticas TI, procesos TI, instancias, indicadores TI)	Revisión de todos los procesos T.I. dos veces al año (líder de procesos ITIL)	Abril - Octubre	SI	En la carpeta dispuesta para alojar la evidencia, no se adjuntó documento alguno sobre el asunto. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: *"Se ha solicitado la actualización de varios formatos, asociado a la solicitud de acceso, el procedimiento para la gestión de cambios, y el Manual para la prestación de los servicios TIC. Esto se evidencia en la resolución 003 del 23 de septiembre de 2024.* *https://educacionbogotamy.sharepoint.com/:b:/g/personal/cbaezb_educacionbogota_gov_co/EQREbcvp6vBDrqTKNiASFfwB1vjYdAlNPdyjwpM28XvHbQ?e=JW5Hot".*	No se reporta evidencia de lo solicitado, que para el caso es del 2023. Aun cuando no está planeada esta actividad en el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SED- MSPI Versión 2 - 2024 dispuesto en la página WEB de la entidad, en el enlace reportado por la OTIC, se aporta la actualización de documentos a través de la RESOLUCIÓN N.º 003 del 23 de septiembre de 2024, donde se incorporan al PROCESO GOBIERNO Y SEGURIDAD DIGITAL, 5 formatos, un manual, un procedimiento, entre otros. Lo anterior permite establecer que la OTIC revisa y actualiza en el Manual de Procesos y Procedimientos de la SED los documentos frutos de la gestión de la OTIC.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
2	Ejecutar la operación de servicios tecnológicos	Informe de seguimiento a la implementación del Plan de continuidad	Junio-Noviembre	PARCIAL	En la carpeta dispuesta para alojar la evidencia, no se adjuntó documento alguno sobre el asunto. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: Durante la vigencia 2023 se inició la elaboración del plan de continuidad del negocio BCP, del cual se presenta soportes en el punto 4.	En el archivo "Evaluación de Riesgos V1", se evidencia la Construcción de Riesgos tecnológicos, dentro de los cuales se contemplan entre otras categorías las software, hardware, infraestructura tecnológica, fluido eléctrico, aires acondicionados, redes y comunicaciones, seguridad, bases de datos, etc. En el archivo "Estrategia de comunicación Plan Continuidad V3", se evidencia Estrategia de Comunicación Plan de Continuidad - Comité de Crisis, en donde se relaciona el Equipo decisorio para la gestión unificada ante una situación de crisis. En el archivo "Formato escenarios y Estrategias de Continuidad V7.0", se evidencia el Procedimiento Gestión de Continuidad de los Servicios TIC, en donde se definen dos tipos de riesgos en tres escenarios diferentes: Actividad Sísmica; Protestas y aglomeraciones, Vandalismo; Incendios. Cada uno de ellos con la identificación del quehacer en las diferentes fases de ejecución, y los planes, procesos y áreas involucradas.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						En el archivo "Formato escenarios y Estrategias de Continuidad V8.0", se encuentra un documento denominado: "Gestión de Continuidad de los Servicios TIC - Estrategias", en donde se relacionan las fases a desarrollar ante un riesgo tecnológico ante un escenario de Virus informático o propagación de malware/ransomware. En el archivo "Formato de Riesgos", se evidencia la construcción de un documento donde se establecen los servicios TI, los riesgos generales, riesgos tecnológicos, riesgos hiperconvergencia; y los diferentes tipos de impacto, según la probabilidad de ocurrencia. En el documento "Plan Continuidad V13", se evidencia la construcción de un documento denominado: Plan de Continuidad de Servicios TIC, de la OTIC a Junio de 2023. Lo anterior, permite concluir que se ha estado elaborando documentación que permita establecer las acciones y estrategias a seguir ante los diferentes riesgos a los que se expone la SED y poder tener un

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						plan de continuidad del negocio, documentos que al consultar en ISOLUCION, en el aplicativo aparecen versiones anteriores de algunos de ellos, razón por la cual es necesario que se terminen de construir, formalizarlos y publicarlos en el aplicativo o en la página WEB, según corresponda.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
3	Ejecutar Inversiones/Compras de T.I. según presupuesto asignado	Informe de ejecución presupuestal	Abril-Julio-octubre	SI	En la carpeta dispuesta para alojar la evidencia, no se adjuntó documento alguno sobre el asunto. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: Se realizan los seguimientos mensuales y la presentación de los informes trimestrales de los proyectos de inversión 7813 y 7949. https://educacionbogotamy.sharepoint.com/:u:/g/personal/cbaezb_educacionbogota_gov_co/Ef9WVxD9mRtOqcRw7w-_llAB4q_8Og7qq4ITxIdjKjknLg?e=g5Dtub https://educacionbogotamy.sharepoint.com/:u:/g/personal/cbaezb_educacionbogota_gov_co/EaTuvqDynHROty5lmTc9SFcBql345FMPSqtnvUvOOV2HHg?e=EaWcxR	No se reporta evidencia de lo solicitado, que para el caso es del 2023. En el enlace reportado por la OTIC se aporta información sobre los seguimientos de los meses de enero a junio de 2024 al proyecto 7813 “Innovación y modernización de la plataforma tecnológica para el mejoramiento de la calidad educativa en los colegios públicos de la ciudad de Bogotá D.C.”, en donde se incluye el estado de la ejecución presupuestal.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
4	Aplicar la gestión integral de proyectos de TI	Matriz de seguimiento a los proyectos de TI (Definir el rol y funciones del Controller)	Marzo - junio - septiembre - Diciembre	SI	En la carpeta dispuesta para alojar la evidencia, no se adjuntó documento alguno sobre el asunto. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: La herramienta de seguimiento de proyectos de Sistemas de Información se actualizó de acuerdo con las necesidades de seguimiento de los proyectos, con el fin de obtener información actualizada del avance en cada una de las etapas y de conocer el estado de cada proyecto. Se incluyeron campos de documentación asociada a los proyectos y de avance en hoja de resumen con el fin de obtener indicadores de seguimiento sobre los proyectos en ejecución. Ver cuadro en Excel reportado presentado en la pregunta 5. Se evidencia archivo en Excel denominado: "Cuadro de seguimiento de Proyectos S.I. 2024"	No se reporta evidencia de lo solicitado, que para el caso es del 2023. En el archivo en Excel denominado: "Cuadro de seguimiento de Proyectos S.I. 2024", se evidencia el seguimiento a 14 proyectos en donde se puede observar el porcentaje de avance de los mismos, las fechas de inicio y fin de los mismos, y el estado en que se encuentran cada uno de ellos. En promedio se tiene un porcentaje real de avance en los 14 proyectos del 74%, pero encontrándose un proyecto con bajo avance en su ejecución, como lo es el de EGD-POA-SISAE (24%), cuya entrega está programada para culminarse en menos de un mes que le queda al proyecto. Así las cosas, es necesario mantener un control sobre los proyectos que desarrolla la OTIC con un seguimiento constante de los mismos y un control sobre los indicadores de ejecución, que permitan su monitoreo y establecer acciones de mejora sobre aquellos que tienen baja ejecución.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
5	Ejecutar el soporte de los sistemas de información	# Informes contratos de servicios	Enero a Diciembre	SI	En la carpeta dispuesta para alojar la evidencia, no se adjuntó documento alguno sobre el asunto. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: Se revisan y firman por las partes los informes de seguimiento al Operador Tecnológico. https://educacionbogotamy.sharepoint.com/:b:/g/personal/cbaezb_educacionbogota_gov_co/ETVKd9Cg9OBGhEbOWLcUQQUBJ4dyUhoaLYXoJZE0nYHJyg?e=BWjZi6 https://educacionbogotamy.sharepoint.com/:b:/g/personal/cbaezb_educacionbogota_gov_co/EcQ5yDKRD5lNpYGWdVl_6ZUBthQCpzTd6qTvWymlphDbyw?e=P4Fnmz En dichos repositorios se evidencia: 1. INFORME DE EJECUCIÓN MENSUAL MESA DE SOLUCIONES Y SERVICIOS DE IT DE ENERO *A MAYO DE 2024* - Contrato N° CO1.PCCNTR.3106464	No se reporta evidencia de lo solicitado, que para el caso es del 2023. Se evidencian informes de seguimiento mensual de enero a mayo de 2024 de la Mesa de Soluciones y Servicios IT del Contrato N° CO1.PCCNTR.3106464

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
6	Aplicar autodiagnóstico de la política de Gobierno Digital	Autodiagnóstico de Gobierno Digital	Junio-Noviembre	SI	En la carpeta dispuesta para alojar la evidencia, no se adjuntó documento alguno sobre el asunto. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: Se realiza seguimiento al FURAG, toda vez que la herramienta del MINTIC fue removida por la entidad mencionada.	A la fecha del seguimiento, consultando el enlace indicado por la OTIC, indicado en la respuesta de la OTIC a la pregunta 6 de este seguimiento, "https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/MEDIR/", se puede observar que el avance de la política de Gobierno Digital se hará, según como se esboza allí: "¿Cómo se hace el seguimiento desde el Ministerio TIC? El seguimiento y evaluación del avance de la Política de Gobierno Digital se realizará con un enfoque de mejoramiento continuo en donde la Dirección de Gobierno Digital del Ministerio TIC, verificará que cada sujeto obligado presente resultados anuales mejores que la vigencia anterior. Para ello, se aplicarán indicadores de cumplimiento e indicadores de resultado, de acuerdo con los criterios de evaluación y seguimiento definidos por el Consejo para la Gestión y Desempeño institucional. Así mismo, se realizarán mediciones de calidad a través del Sello de Excelencia de Gobierno Digital.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						En el archivo descargable del Manual de Gobierno Digital, se presentan los indicadores que serán aplicados a cada entidad pública". Al intentar abrir el autodiagnóstico específico en materia de seguridad y privacidad de la información dispuesto en la página WEB del MINTIC no permite el ingreso él. Por lo anterior, no es posible verificar cómo se desarrolló el autodiagnóstico de la política de Gobierno digital en la vigencia 2023 según herramientas del MINTIC, como la manifiesta la OTIC. Ahora bien, consultando el tablero interactivo de Gobierno Digital del MINTIC, la entidad en sus resultados generales cumple en un 84,8 % en su índice de Gobierno Digital, sobrepasando el 82,2 % del promedio del grupo par, sin embargo, se detallan acciones de mejora en 8 de los 10 subíndices de Gobierno Digital para la entidad sobre la materia, que es necesario implementar en la SED, dado que se cumple con el 100% en solo dos de los 10. Es importante mencionar que en el de Servicios Ciudadanos Digitales el avance es solo de un 14,3%, por

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						lo que se deben establecer mecanismos que permitan evidenciar avances en dicho indicador.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
7	Definir la Estrategia de Uso y apropiación de TIC en la entidad.	Informe de diagnóstico (abril) y resultados de la estrategia (noviembre) de uso y apropiación.	Marzo - Diciembre	PARCIAL	Documentos denominados: 1. Informe_Plan Capacitaciones_OTIC_2SEM2023_FINAL, titulado: INFORME DE ESTRATEGIA DE USO Y APROPIACION PARA LOS PROYECTOS T.I.PLAN DE CAPACITACIONES 2023 Y DIVULGACIÓN DE LA POLITICA DE GOBIERNO Y SEGURIDAD DIGITAL Segundo semestre 2023. 2. 2023_Gobierno_númeral7y8-item7	1. Se evidencia informe en el que se relacionan las capacitaciones realizadas en el 2023 en temas de TI con el fin de apoyar el conocimiento de herramientas tecnológicas, los marcos de referencia, principios generales y recomendaciones sobre Seguridad Digital para los tres niveles de la Secretaría de Educación del Distrito, con la colaboración de la Dirección de Talento Humano y la Dirección de Ciencias, Tecnologías y medios educativos. En él se puede observar que, basados en el análisis de resultados de la encuesta adelantada por la Dirección de Talento Humano en diciembre 2023 para 691 servidores incluido Rectores, los dos aspectos más importantes que los funcionarios consideran son: * Estrategias y herramientas para gestionar, administrar y estructurar el conocimiento. * Procesamiento de datos e información, analítica de datos y administración y gestión de datos e información. 2. Frente la pregunta sobre Gobierno Digital en el FURAG: "7.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						¿Qué acciones se han llevado a cabo para desarrollar las oportunidades de mejora relacionadas en el informe de auditoría al Proyecto de Inversión 7813 modernización de la plataforma tecnológica para el mejoramiento de la calidad educativa y ¿cuáles han sido los avances presentados al plan de mejoramiento frente a los hallazgos/observaciones, identificados en el proceso auditor?", la misma dependencia indica sobre el ítem: "Definir la Estrategia de Uso y apropiación de TIC en la entidad", que su cumplimiento fue "PARCIAL", en cuanto al Informe de diagnóstico (abril) y resultados de la estrategia (noviembre) de uso y apropiación.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
8	Implementar servicios digitales, desarrollados bajo tecnologías web que permita dar respuesta al ciudadano en sus trámites y servicios ante la entidad	Realizar la interoperabilidad con la Cancillería Colombiana para el servicio de apostillaje de título de bachillerato	Enero - marzo	SI	1. Se adjunta trazabilidad de los correos con la Cancillería, desde el lunes, 04 de diciembre de 2023 hasta el 09 de enero de 2024, con Asunto: RE: FUT - Legalización Documentos al Exterior, según radicado No: F-2023-18626, en donde se informa que, con respecto a las reuniones sostenidas entre las dos entidades, la SED ya realizo el paso a producción de los ajustes trabajados. Se envía End-Point de conexión con el apuntamiento a producción. Radicado de prueba en producción: Radicado: F-2024-3775 Código de verificación: DGOKB 2. La OTIC a través del radicado I-2024-113445 enviado a la OCI reporta que: Desde el 15 de enero de 2024, se encuentra funcionando, debido a diversos ajustes al requerimiento de la interoperabilidad con Cancillería para el servicio de apostillaje. La Apostilla o Legalización en Línea se solicita a través del sitio web del Ministerio de Relaciones Exteriores en https://tramites.cancilleria.gov.co/apostillalegalizacion/solicitud/inicio.aspx opción “Documentos electrónicos con firma digital - Secretaría de Educación de Bogotá”, seleccionando el país de destino e ingresando el radicado de solicitud FUT.	Al acceder al enlace enviado por la OTIC, se puede acceder al sitio de la cancillería: https://tramites.cancilleria.gov.co/apostillalegalizacion/solicitud/inicio.aspx, en donde, al ingresar en Documento o Entidad: Secretaría de Educación de Bogotá, se indica que: *"Por esta opción apostille o legalice los documentos certificados por la Secretaría de Educación de Bogotá. Tenga en cuenta que debe indicar el radicado y el código de verificación que se encuentra en la certificación emitida por esa Secretaría".*

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
9	Definir el modelo de Gobierno de TI	Política de TI	Mayo	PARCIAL	Adjunta "manual para la prestación de servicios TIC"	La oficina de tecnologías de información y comunicación ha construido el "manual para la prestación de servicios TIC" como un esfuerzo significativo en búsqueda de establecer pautas para el correcto uso de herramientas informáticas en la entidad y en línea con las disposiciones establecidas en el numeral 5.2 de la NTC ISO 270001 , dicho documento se centra principalmente en aspectos operativos y técnicos y aunque no posee un enfoque estratégico dispone de orientaciones para el correcto uso de TI dentro de la entidad. El documento fue aprobado por la oficina asesora de planeación ya que bajo su consideración no es necesaria la construcción de una política de tecnologías de la información. Sin embargo, es importante mencionar que la resolución 500 de 2021 del MINTIC, establece que: “ARTÍCULO 5. La estrategia de seguridad digital. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios,

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue….Y que dicha estrategia debe ser aprobada a través de un acto administrativo de carácter general". Adicionalmente los lineamientos para el MSPI impartidos por MINTIC "Documento Maestro del Modelo de Seguridad y Privacidad de la Información de MINTIC" establecen que "Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						desempeño", en consonancia con el compromiso que la Ley asigna a la Alta Dirección en temas de seguridad informática. Por lo tanto, es necesario asegurar que las políticas relacionadas con el MSPI que se encuentran publicadas en el portal web de la entidad sean, en primera instancia, avaladas por el Comité Institucional de Gestión y Desempeño, y respaldadas mediante acto administrativo que manifieste la voluntad de la alta dirección, ya que afectan el funcionamiento interno de la entidad y se debe procurar su apropiación por parte de funcionarios y contratistas.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
10	Actualizar las políticas asociadas al MSPI y socializarlas	2 políticas actualizadas y socializadas	Junio-diciembre	PARCIAL	Enlaces página web de la entidad " Políticas y lineamientos sectoriales e institucionales - Oficina de Tecnologías de la Información y las Comunicaciones", en donde se evidencia publicación de políticas asociadas al MSPI	Se evidencia el cumplimiento parcial a la actividad “Actualizar las políticas asociadas al MSPI y socializarlas”, pues si bien la OTIC publicó en la web de la entidad la “política de datos personales”, la “política de privacidad y condiciones de uso de portales web” , la “política de uso y manejo del correo electrónico "y la “política de privacidad y seguridad en la información”; la única de estas que fue debidamente formalizada, fue la “política de privacidad y seguridad en la información” , emanada mediante acto administrativo, Resolución 1944 de 2016, sin embargo, los otros instrumentos orientativos no se encuentran publicados en el sistema de gestión de la entidad, ni representan la voluntad formal de la alta dirección, pues no han sido publicados como actos administrativos, tampoco se evidencia su aprobación por otras instancias en la entidad, diferentes a la oficina de tecnologías de la información. En este punto es importante mencionar que los lineamientos para el MPSI impartidos por MINTIC y el marco

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						normativo bajo el cual se desarrolla el presente seguimiento refieren que “Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño” , en consonancia con el compromiso que la Ley asigna a la alta dirección en temas de seguridad informática , así las cosas , se hace necesario evidenciar que las políticas relacionadas y publicadas en el portal web de la entidad, sean en primera instancia avaladas por el comité institucional de gestión y desempeño, debidamente publicadas en el sistema de gestión y respaldadas mediante acto administrativo que manifieste la voluntad de la alta dirección ya que afectan el funcionamiento interno de la entidad y se debe procurar su apropiación.

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
11	Ejecutar plan de tratamiento de riesgos y evaluación de los controles de seguridad	Informe de seguimiento al plan de tratamiento de riesgos	Enero a Diciembre	SI	Las evidencias de seguimiento, aplicación de controles y análisis de gestión del riesgo se encuentran ubicados en el SharePoint del equipo de seguridad digital	Cumple
12	Actualizar el Autodiagnóstico del estado actual del Modelo de Seguridad y Privacidad de la información	Autodiagnóstico del estado actual del Modelo de Seguridad y Privacidad de la información	Junio	SI	Adjunta "AUTODIAGNOSTICO MSYPI" en formato Excel desarrollado bajo la herramienta que dispuso el MINTIC para dicho propósito	El diagnostico muestra un nivel de madurez inicial del MSPI
13	Actualizar mapa de riesgos	Mapa de riesgos actualizado	Abril	SI	Presenta mapa de riesgos	La resolución No 5 del 24 de diciembre de 2021 establece que la actualización del mapa de riesgos de seguridad digital debe realizarse a más tardar el 30 de abril de cada vigencia por parte de la segunda línea de defensa, que para el caso es la OTIC. Se evidencia el mapa de riesgos se encuentra debidamente

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
						formalizado en el sistema de gestión de la entidad y publicada la correspondiente a la vigencia, en donde se incluye la actualización de los activos de información de los procesos de la SED.
14	Revisar y actualizar plan de tratamiento de riesgos de seguridad y privacidad de la información	Plan de tratamiento de riesgos de seguridad y privacidad de la información	Febrero-abril	SI	Presenta plan de tratamiento de riesgos de seguridad digital 2023-2024	Cumple
15	Seguimiento al contrato de implementación de protocolo IPV6	Informe de implementación	Marzo - octubre	NO	No presenta evidencia	Contrato SED-LP-REDP-008-2022 no están cargadas las evidencias de ejecución
16	Campaña de sensibilización para directivos, funcionarios y usuarios sobre IPV6 y la transición	Informe de campaña de sensibilización	Abril-septiembre	NO	No presenta evidencia	Contrato SED-LP-REDP-008-2022 no están cargadas las evidencias de ejecución

No	ACCION	PRODUCTO	CRONOGRAMA	CUMPLIMIENTO	Evidencias OTIC	Revisión OCI
	realizada en la entidad					
17	Pruebas de pentesting portal Secretaría de Educación https://www.educacionbogota .edu.co/	Informe de seguridad, aplicación y/o mejoras en los controles de seguridad aplicados	Marzo -julio- Noviembre	SI	Presenta informe de seguridad en los servicios publicados en los dominios .edu y .gov	Cumple