ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

MEMORANDO

Radicado Nº I-2022-115761
Fecha: 31-10-2022 - 11:30
Folios: 1 Anexos: 12
Radicador: ANDREA CAROLINA HERNANDEZ PARDO - 1200
Destino: 1700 - OFICINA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
Consulte el estado de su trámite en www.educacionbogota.edu.co opción CONSULTA TRÁMITE con el codigo de verificación: OO8BQ

PARA: Wilson Adiel Rodriguez Rodriguez
Jefe Oficina de tecnologías de la información

DE: Jefe Oficina de Control Interno

ASUNTO: Informe Seguimiento Seguridad Digital 2022

Fecha: 31 de octubre de 2022

Respetado doctor Wilson,

En atención al plan de seguimiento que adelantó esta Oficina al proceso de seguridad digital, cuyo objetivo fue: “Verificar la implementación de controles establecidos en el mapa de riesgos de seguridad digital 2022 y la política de Seguridad Digital de la dimensión 3 “Gestión con valores para resultados” del Modelo Integrado de Planeación y Gestión – MIPG”, me permito remitir el informe resultado de dicho seguimiento.

Por tratarse de una actividad de seguimiento que adelantó la Oficina de Control Interno, es importante mencionar que NO se requiere formulación de plan de mejoramiento y es preciso tener en cuenta las recomendaciones incluidas en el informe, para el fortalecimiento del proceso de seguridad digital en la SED.

Agradezco la colaboración ofrecida por el equipo de trabajo archivo SED en el desarrollo de este seguimiento y le invito a contar con nuestro apoyo en el cumplimiento de los planes y acciones para la mejora continua de la seguridad digital en la entidad.

Cordial saludo,

OSCAR ANDRES GARCIA PRIETO
Jefe Oficina de Control Interno

Firmado digitalmente por OSCAR ANDRES GARCIA PRIETO
Nombre de reconocimiento (DN): title=JEFE DE OFICINA CODIGO 006 GRADO 06, sn=GARCIA PRIETO, street=AC 26 66 63, st=BOGOTA D.C., ou=BANCO DE LA REPUBLICA SEC - 1 AN, serialNumber=1673427, 1.3.6.1.4.1.23267.2.3=8999990619, 1.3.6.1.4.1.23267.2.2=79969752, 1.3.6.1.4.1.23267.2.1=15, o=SECRETARIA DE EDUCACION DEL DISTRITO, l=BOGOTA D.C., givenName=OSCAR, email=OGARCIAP@EDUCACIONBOGOTA.GOV.CO, c=CO, cn=OSCAR ANDRES GARCIA PRIETO

Proyectó: Andrea C Hernández P- Camilo A Cruz G Juan F Rodríguez F
Profesionales OCI
Anexo: Informe de seguimiento (12 folios)

I. IDENTIFICACIÓN DE LA AUDITORÍA	
Auditor(es)	1. Camilo Andrés Cruz González 2. Andrea Carolina Hernández Pardo 3. Juan Francisco Rodríguez Fernández
Proceso auditable	12. Gobierno y Seguridad Digital
Código PAA / Dependencia	PAA: No.56 -2022 Dependencia: 1700- Oficina de Tecnologías de la Información y las Comunicaciones
Objetivo General	Verificar la implementación de controles establecidos en el mapa de riesgos de seguridad digital 2022 y la política de Seguridad Digital de la dimensión 3 “Gestión con valores para resultados” del Modelo Integrado de Planeación y Gestión - MIPG.
Alcance	El seguimiento se realizó a la gestión adelantada por la Oficina de Tecnologías de la Información y las Comunicaciones (antes REDP) 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 comprenderá del 16 de septiembre de 2021 al 01 de septiembre de 2022.

II. INFORME EJECUTIVO

El seguimiento realizado se abordó desde la revisión de las evidencias presentadas por la Oficina de Tecnologías de la Información y las Comunicaciones, de aquí en adelante OTIC, para la gestión de riesgos de seguridad digital 2021 y 2022. Se llevaron a cabo revisiones tanto de la aplicación de la metodología de administración de riesgos para seguridad digital en su versión 01 de fecha 24 de diciembre de 2021 como de la ejecución de los controles del anexo A de la norma ISO 27001 establecidos y aplicados por la Entidad para cada uno de los riesgos identificados y el seguimiento a la resolución No 746 de 2022.

De la revisión efectuada, los aspectos más importantes son los siguientes:

Se evidencia avance en la identificación de riesgos de seguridad digital, en especial para el proceso de Gobierno y Seguridad Digital como se define en el alcance del Plan de Tratamiento de Riesgos de la vigencia 2022, sin embargo, se debe realizar el proceso de identificación para todos los activos de información existentes en los procesos. La matriz de riesgos de seguridad digital de la presente vigencia contiene identificación de riesgos solo para activos de información de tipo software, así que se debe realizar la identificación de riesgos de seguridad digital en los 22 procesos de la Entidad. La OTIC como segunda línea de defensa y responsable de brindar lineamientos y asesoría debe continuar el acompañamiento a cada uno los procesos para la identificación y valoración de los riesgos de seguridad digital.

De la ejecución de los controles del Anexo A de la norma ISO 27001 establecidos en la matriz de riesgos de Seguridad Digital (15 controles), se encontró que en el 80% (12 controles) las evidencias presentadas guardan relación con la estrategia de control propuesta por la Entidad para la mitigación de los riesgos, el 20% (3 controles) restante debe fortalecer la ejecución de las actividades descritas.

Con relación a la aplicación de lo establecido en la resolución 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones, desde la OTIC se han adelantado acciones para dar cumplimiento a

la resolución, considerando que es necesario adelantar y fortalecer actividades de socialización de las políticas de tratamiento de datos personales y relación con proveedores, así como soportar los controles de protección de privacidad en aquellos sistemas asociados con el tratamiento de datos personales.

III. RESULTADOS

1. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La Entidad mediante resolución 005 del 24 de diciembre de 2021 "Por la cual se modifica el mapa de procesos de la SED, se adoptan las caracterizaciones de los procesos que lo componen y se dictan otras disposiciones", adoptó la caracterización del proceso 012-CP-001 "Gobierno y Seguridad Digital" y se asociaron los documentos existentes al nuevo proceso, dentro de los cuales se encuentra la Metodología de Administración para la Gestión de los Riesgos de Seguridad Digital versión 1 del 24 de diciembre de 2021, que dentro de su alcance establece "(…) *la administración del riesgo de seguridad digital debe ser extensible y aplicable a los procesos de la entidad de acuerdo con los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información definidos por el MINTIC*".

Una vez revisada la aplicación de la metodología vigente en la matriz de riesgos de seguridad digital para la vigencia 2022 se encontró lo siguiente:

Para los tres riesgos inherentes de seguridad digital: pérdida de confidencialidad, pérdida de integridad y pérdida de la disponibilidad, se identificaron 52 activos de información de tipo software, asociados a 13 procesos de la Entidad con la siguiente valoración de criticidad:

Tabla No.1 Activos de información identificados

Activos de Información Identificados	Criticidad Activo	Proceso
Construcciones Project Online	ALTA	Acceso y Permanencia Escolar
Construcciones	BAJA	Acceso y Permanencia Escolar
Sistema de Inventarios SAE SAI – NVC	BAJA	Acceso y Permanencia Escolar
Gestión de Cobertura – APEX	BAJA	Acceso y Permanencia Escolar
Movilidad Escolar	BAJA	Acceso y Permanencia Escolar
Alertas	BAJA	Articulación Interinstitucional
Sistema de Apoyo Escolar	BAJA	Calidad Educativa Integral
Sistema Seguimiento a Egresados	BAJA	Calidad Educativa Integral
Si me conoces - Primera Infancia	BAJA	Calidad Educativa Integral
SVDI - Sistema Integral de Valoración Infantil	BAJA	Calidad Educativa Integral
Si me conoces – Monitoreo	BAJA	Calidad Educativa Integral
Si me conoces - Jornada Única	BAJA	Calidad Educativa Integral
Evaluación Docente	BAJA	Calidad Educativa Integral
Suma de Sueños	BAJA	Educación Inclusiva

Servicios públicos	BAJA	Gestión Administrativa
Arrendamientos	BAJA	Gestión Administrativa
Gestión de Contratos	BAJA	Gestión Contractual
IFindIt	BAJA	Gestión Documental
PS Documents	BAJA	Gestión Documental
Apoteosys	BAJA	Gestión Financiera
Matriz CHIP (Contable)	BAJA	Gestión Financiera
SI CAPITAL FSE	BAJA	Gestión Financiera
Matriz CHIP (Presupuestal)	BAJA	Gestión Financiera
Instituciones	BAJA	Gobierno y Seguridad Digital
SAETA	BAJA	Gobierno y Seguridad Digital
Dexon	BAJA	Gobierno y Seguridad Digital
SIAI - Sistema Integrado de Acceso e Ingreso	BAJA	Gobierno y Seguridad Digital
SIARA - Sistema de Investigaciones Administrativas y Recursos de Apelación	BAJA	Inspección y Vigilancia del Servicio Educativo
POA - Plan Operativo Anual	BAJA	Planeación Estratégica
DUEB - Directorio Único de establecimientos Educativos de Bogotá	BAJA	Planeación Estratégica
Isolucion	BAJA	Planeación Estratégica
Servicio al ciudadano	BAJA	Servicio Integral a la Ciudadanía
SIGA	BAJA	Servicio Integral a la Ciudadanía
Digiturno	BAJA	Servicio Integral a la Ciudadanía
FUT - Formulario Único de Trámites	BAJA	Servicio Integral a la Ciudadanía
Consulta Diplomas	BAJA	Servicio Integral a la Ciudadanía
Humano	BAJA	Talento Humano
Recobro de incapacidades docentes	BAJA	Talento Humano
Documentos Seguros	BAJA	Talento Humano
Escalafón	BAJA	Talento Humano
Tiempo de Servicios Docentes Privados	BAJA	Talento Humano
KOMBO	BAJA	Talento Humano
Audiencia Docente	BAJA	Talento Humano
Traslados docentes	BAJA	Talento Humano
Planta	BAJA	Talento Humano
Certificados Historia Laboral	BAJA	Talento Humano
IMAG - Información del Magisterio de la SED	BAJA	Talento Humano
Reubicaciones administrativas	BAJA	Talento Humano
Selección de docentes provisionales	BAJA	Talento Humano
INFOMAG - Fondo Prestacional del Magisterio	BAJA	Talento Humano
Encargos Directivos Docentes	BAJA	Talento Humano
Fondo de Ahorro y Vivienda Distrital	BAJA	Talento Humano

Fuente: Elaboración equipo auditor – Matriz de Riesgos de Seguridad Digital 2022

De acuerdo con la metodología vigente, la identificación de activos de información debe realizarse en cada uno de los procesos, estableciendo lo que se debe proteger bajo los términos de seguridad de la información de acuerdo con su clasificación o naturaleza como: información, software, hardware, componentes de red, servicios intangibles, personas e instalaciones, entre otros.

Por otra parte, el documento Plan de Tratamiento de Riesgos de Seguridad Digital para la vigencia 2022 establece dentro de su alcance “El presente plan de riesgos tiene alcance para el proceso de Gestión de Tecnologías de Información y Comunicaciones, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información, habilitador transversal de la Política de Gobierno Digital expedida por el MINTIC.”, en dicho documento solo se mencionan como activos de información del proceso, el inventario de sistemas de información de la Entidad, dejando de proteger los demás tipos de activos descritos anteriormente que se pueden identificar en este proceso y que están relacionados con componentes de TI.

Así mismo contrastada la información de los sistemas de información relacionados en el Plan de Tratamiento de Riesgos y la Matriz de Riesgos de Seguridad Digital, con el inventario de sistemas de información entregado por la OTIC como soporte (Catálogo público 22Abr2022.xlsx), se encontró una diferencia de 4 sistemas de información (faltantes en los documentos de gestión de riesgos), los cuales se relacionan a continuación:

Tabla No.2 – Diferencias sistemas de información

NOMBRE	CATEGORIA
Cierre de Brechas Digitales	Misional
Reto A la U	Estratégico
Jóvenes A la U	Estratégico
SACE-Sistema de Alianzas y Cooperación Escolar	Estratégico

Fuente: Elaboración equipo auditor - Inventario de sistemas de información presentado por la OTIC

Cabe anotar que el documento Plan de Tratamiento de Riesgos de Seguridad Digital de fecha enero de 2022 debe ser actualizado con lo dispuesto en la resolución No. 005 de 2021, en lo referente al nombre del proceso (Gestión de Tecnologías de Información y Comunicaciones por Gobierno y Seguridad Digital) y en la versión y fechas de los documentos asociados al mismo.

Con respecto a la valoración del diseño de controles donde se establece que se debe tener en cuenta en la redacción del control las variables de: responsable, periodicidad, propósito, como se realiza la actividad del control, manejo de las observaciones o desviaciones y evidencia, se encontró lo siguiente:

Del anexo A de la norma ISO 27001 se seleccionaron 15 controles para ser aplicados a los riesgos identificados para cada uno de los activos de información asociados, para un total de 260 registros en la matriz de seguridad digital:

Tabla No.3 Controles implementados Anexo A ISO 27001

Control	Nombre	Descripción
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y

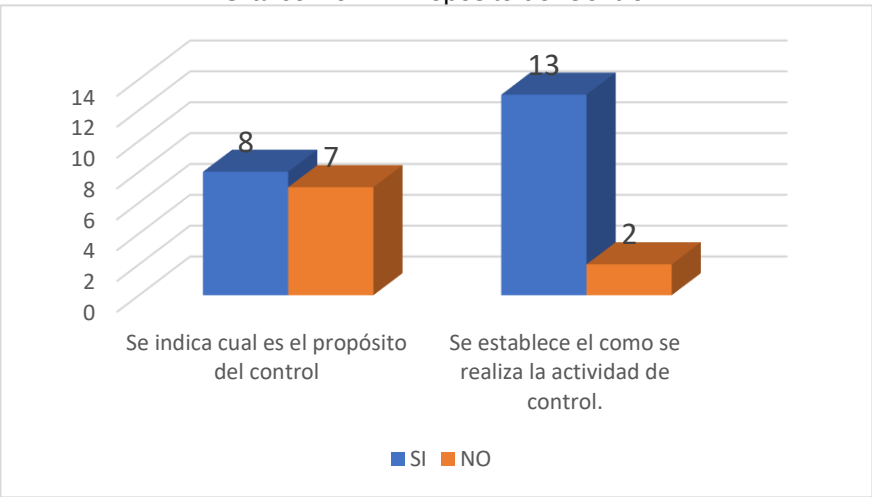
		ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Fuente: Elaboración equipo auditor – Matriz de riesgos de seguridad digital

El 100% de los controles cuentan con un responsable del control, que está definido como “líder técnico”. De otra parte, no se puede identificar en ninguno de los controles, el tratamiento de las desviaciones u observaciones de la ejecución y la periodicidad (la matriz cuenta con espacios de frecuencia e implementación ambos con opciones de Manual o Automático).

En cuanto al propósito de control, en el 53% correspondiente a 8 controles se describe el propósito; el 47% restante corresponde a los controles A6.1.1, A6.1.5, A8.1.3, A9.3.1, A11.1.3, A12.1.1 Y A13.2.4, para la descripción de la actividad de control en el 87% se describe cómo se realiza, los dos controles faltantes corresponden a A6.1.1 y A7.1.1.

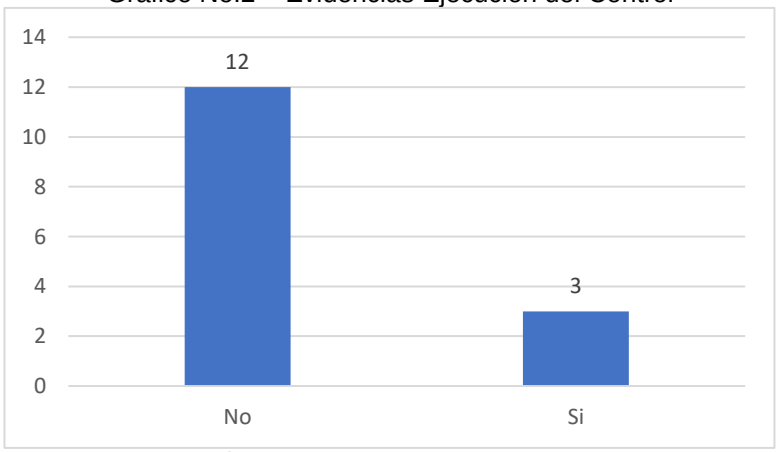
Gráfico No. 1 - Propósito del Control



Fuente: Elaboración equipo auditor - Evidencia presentada por la OTIC

Respecto de la evidencia de la ejecución de los controles, en 12 de ellos no se identifica esto de forma clara y especifica y la evidencia tiene coherencia con la actividad de control definida en los 3 controles restantes. Las falencias en la definición de la evidencia se presentan en los controles A5.1.1, A6.1.1, A8.1.3, A9.2.2, A9.3.1, A9.4.1, A11.1.3, A12.1.1, A13.1.2, A13.2.4, A14.1.3 Y A17.2.1.

Grafico No.2 – Evidencias Ejecución del Control



Fuente: Elaboración equipo auditor - Evidencia presentada por la OTIC

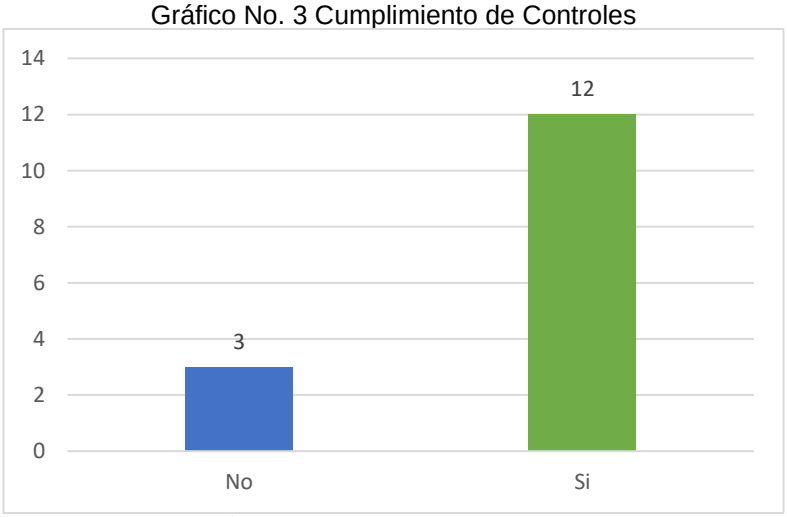
2. APLICACIÓN DE CONTROLES ANEXO A ISO 27001

El seguimiento a la ejecución de los controles adelantado por la Oficina de Control Interno correspondió a la verificación de soportes de las actividades de control descritas como estrategia de aplicación del Anexo A de la norma ISO 27001, donde la SED seleccionó 15 controles de los 114 relacionados en dicha norma.

Las evidencias fueron dispuestas por la OTIC con la información relacionada para cada uno de los controles aplicados por la Entidad, encontrando lo siguiente:

Con respecto a la coherencia de las evidencias presentadas como ejecución de los controles establecidos, en el 80% que equivale a 12 controles (A5.1.1, A6.1.1, A6.1.5, A7.1.1, A7.2.2, A8.1.3, A9.2.2, A9.3.1, A12.1.1, A13.1.2, A13.2.4 y A17.2.1) los soportes guardan relación con lo descrito en la estrategia, para el 20% restante no corresponde a la actividad del control ejecutado.

Gráfico No. 3 Cumplimiento de Controles



Fuente: Elaboración equipo auditor - Evidencia presentada por la OTIC

A continuación, se presentan las observaciones adicionales de la Oficina de Control Interno resultado de la verificación de las evidencias que soportan la ejecución de los controles.

A9.4.1 - Hacer cumplir el registro de auditoría detallado para acceder a datos confidenciales o cambios en datos confidenciales (utilizando herramientas como File Integrity Monitoring o Información de seguridad y monitoreo de eventos).

En el seguimiento de la OTIC se menciona la aplicación de la herramienta de monitoreo Whatsup Gold, al solicitar reportes para verificar el monitoreo de la herramienta, se remiten reportes diarios y semanales programados en la herramienta para el monitoreo de la disponibilidad de los canales y servicios. No se presentan soportes de monitoreo de eventos o logs, como se describe en el control.

La OTIC informa que la herramienta tiene licencia de funcionamiento desde el 31 de diciembre de 2021 y que a la actualidad se está realizando la renovación de las licencias.

A11.1.3 "Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones"

Se presenta como evidencia el catálogo del sistema de acceso, pero este documento no es evidencia de la implementación y ejecución del control.

A14.1.3 - Implemente herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas esté ejecutando las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.

La evidencia muestra que el System Center Configuration Manager – SCCM con que cuenta la Entidad, no está realizando actualizaciones de software de terceros, que es el propósito del control establecido. El software solo está desplegando las actualizaciones para los productos de Microsoft.

De otra parte y con el fin de fortalecer la ejecución de los controles donde la evidencia si guarda coherencia con lo establecido en la estrategia de ejecución, la Oficina de Control Interno presenta las siguientes recomendaciones:

A5.1.1 - Defina políticas de seguridad de la información claras y alineadas con los objetivos corporativos y cuyo alcance garantice el cumplimiento legal.

Los soportes muestran que se encuentran definidas las políticas de: uso y manejo del correo electrónico, privacidad y condiciones de uso de portales web, uso de dispositivos móviles en la redes institucionales y protección de los datos personales. Es preciso que desde la OTIC se fortalezca las actividades de socialización y apropiación de las políticas de seguridad digital a los funcionarios en los tres niveles de la SED y desde el rol como segunda línea de defensa, realizar seguimiento a la implementación y aplicación de las políticas relacionadas para evitar la materialización del riesgo asociado al control.

7.2.2. - Se deberán definir programas de toma de conciencia (campañas, folletos, boletines, etc.), estas deberán contemplar: * la necesidad de familiarizarse con las reglas y obligaciones de seguridad de la información aplicables y de cumplir con ellas. * la rendición personal de cuentas, por las acciones y omisiones propias, y las responsabilidades generales con relación a asegurar o proteger la información. * los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información). * los puntos de contacto y los recursos para información adicional y asesoría sobre asuntos de seguridad de la información. * Capacitar al personal técnico y de desarrollo en la identificación de parámetros técnicos que pueden divulgar información relacionada con la tecnología empleada.

La OTIC presentó como soporte el informe de estrategia de uso y apropiación para los proyectos T.I. en donde se evidencia el plan de capacitaciones en seguridad de la información 2022, relacionados con ciber riesgos, seguridad digital, aplicaciones y política de tratamiento de datos personales. Es pertinente fortalecer las socializaciones a los funcionarios en cuanto a las políticas y procedimientos relacionados al proceso de seguridad digital, en pro de mejorar la toma de conciencia en el manejo y protección de los activos de información que dispone actualmente la SED.

A13.1.2 - * Se debe implementar canales de trasmisión redundantes, lo cual implica redundancia de equipos de comunicación y definición de protocolos de redundancia. * Defina arquitectura de los sistemas en alta disponibilidad HA. * Defina niveles de servició con los proveedores de comunicación. * Evalué la red regularmente a fin de identificar programas maliciosos de interceptación y manipulación de información.

Para verificar la ejecución del control se realizó a la OTIC solicitud adicional de soportes de la ejecución de los procedimientos 12-PD-023 Gestión de la Continuidad de Servicios de TIC y Administración de Crisis y 12-PD-022 Gestión de la Continuidad de Servicios TIC Fase preventiva, en especial lo relacionado con: aprobación y socialización de los documentos "Políticas de Continuidad de Servicios TIC", "Plan de Continuidad de Servicios TIC", "Plan de pruebas de la continuidad de los Servicios TIC" e informe de las pruebas funcionales realizadas.
Como respuesta la OTIC informó que los documentos se encuentran en elaboración y a la espera de ser presentados al jefe para aprobación y posterior paso a la Oficina Asesora de Planeación para revisión y publicación.

Es importante que desde la OTIC se prioricen los esfuerzos necesarios para que el trámite de esta documentación clave para el proceso de Gobierno y Seguridad Digital se realice a la mayor brevedad posible, ya que en dichos documentos se definen los lineamientos necesarios para evitar impactos significativos en la continuidad del negocio y tener una respuesta oportuna a posibles interrupciones.

3. SEGUIMIENTO A LA APLICACIÓN DE LA RESOLUCIÓN NO 746 DEL 11 DE MARZO DE 2022

Se efectuó una revisión documental con corte al 1 de septiembre de 2022, con el fin de realizar seguimiento a la aplicación de la Resolución No. 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones "*Por el cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021*".

Producto del análisis se extraen las siguientes conclusiones:

La OTIC aportó documento de la política de tratamiento de datos personales cuya vigencia rige a partir de agosto del 26 de agosto de 2022, sin embargo, dicho documento no se encuentra actualizado en la sección de la página web de la Entidad: "Políticas de seguridad de la información del sitio web y protección de los datos personales". Adicionalmente es pertinente fortalecer las jornadas de socialización en los tres niveles de la SED de la política, considerando la actualización realizada en agosto de 2022, esto con el fin de que esta sea apropiada por todos los funcionarios y colaboradores de la SED.
Es importante también, realizar seguimiento y monitoreo a la aplicación de la política de tratamiento de datos personales en los tres niveles de la SED y los procedimientos vigentes relacionados al control de acceso.

Durante el seguimiento se evidenció que mediante la Resolución 2256 del 1 de agosto de 2022 de la SED, se estableció el rol de asesor de protección de datos personales, en atención a la necesidad de garantizar la protección de datos personales en la SED, se hace necesario que en conjunto con el equipo de gobierno y seguridad digital se realicen y fortalezcan procesos de evaluación y medición de los resultados de la gestión adelantada, con relación a la protección de los datos personales como un mecanismo de autocontrol y se visibilice el accionar tanto del asesor como del equipo de seguridad digital al interior de la SED.

Atendiendo a lo establecido en la Resolución No 746, es pertinente que se soporten los controles de protección de privacidad en los sistemas de información identificados en el inventario y que estén relacionados con el tratamiento de datos personales, así mismo se debe continuar fortaleciendo las medidas adoptadas al momento de adquirir productos y servicios de Seguridad Digital operados en entornos de nube.

Con respecto a la política de relación con proveedores, se debe formalizar, publicar y socializar el documento presentado por la OTIC como soporte, así como hacer seguimiento al cumplimiento de los lineamientos que allí se establecen por los responsables de la aplicación de la política (Proveedores y terceros de la SED, Supervisores de Contrato y Equipo de Gobierno y Seguridad Digital).

Por último, de acuerdo con lo establecido en la resolución 746 de 2022 con relación al artículo 6.1 gestión de la seguridad de la información para las relaciones con proveedores en su numeral 3 “analizar los riesgos de seguridad digital propios de la integración de soluciones e implementar controles para su mitigación”, se debe revisar la definición del riesgo de seguridad digital, incluido dentro del documento de los estudios previos aportado por la OTIC, donde se evidencia la descripción del riesgo como un control, tal como se observa en la siguiente imagen:

Imagen No.1 Descripción riesgo seguridad digital

Seguridad digital	Exigir al contratista suscripción del acuerdo de confidencialidad	Posible	Bajo	0.70%	La supervisión del contrato deberá garantizar la firma del acuerdo de confidencialidad cuando el proveedor tenga accesos a datos personales, privados y/o sensibles.		x	Ajustar el acuerdo de confidencialidad con relación a la necesidad.

Fuente: Evidencia presentada por la OTIC – Documentos estudios previos componente, certificados y firmas digitales 2022

4. ESTADO ACCIONES PLANES DE MEJORAMIENTO SEGURIDAD DIGITAL

Producto de las auditorias de Seguridad Digital en las vigencias 2020 y 2021, realizadas desde la Oficina de Control Interno, se suscribieron dos planes de mejoramiento en donde se formularon 31 acciones de mejora para el año 2020 y 3 acciones de mejora para el 2021.

El estado de las acciones de mejora es el siguiente:

Gráfico No. 4 Planes de mejoramiento Seguridad Digital

Fuente: Elaboración equipo auditor

La acción de mejora propuesta que se encuentra vencida pertenece al hallazgo No. 372 de la auditoria vigencia 2020.

Lo anterior se puede corroborar en el último seguimiento que realiza la Oficina de Control Interno a los planes de mejoramiento con corte a 30 de septiembre de 2022.

IV. CONCLUSIONES

Producto de la verificación realizada por el equipo auditor y las evidencias presentadas por la OTIC se presentan las siguientes conclusiones:

1. La matriz de riesgos de seguridad digital 2022 demuestra que se viene avanzando en la identificación de riesgos y controles; sin embargo, se debe fortalecer el ejercicio aplicando la metodología vigente de administración de riesgos de seguridad digital a los 22 procesos existentes (Estratégicos, misionales, de apoyo y de evaluación). Lo anterior con el fin de cubrir los diferentes tipos de activos de información (información, software, hardware, componentes de red, servicios intangibles, personas e instalaciones) que afecten el desempeño de la SED en las dimensiones de integridad, disponibilidad y confidencialidad.

2. De la ejecución de los controles del Anexo A de la norma ISO 27001 establecidos en la matriz de riesgos de Seguridad Digital (15 controles), se encontró que en el 80% (12 controles) las evidencias presentadas guardan relación con la estrategia de control propuesta por la Entidad para la mitigación de los riesgos, el 20% (3 controles) restante debe fortalecer la ejecución de las actividades descritas.

3. Con relación a la aplicación de lo establecido en la resolución 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones, desde la OTIC se han adelantado acciones para dar cumplimiento a la resolución, no obstante, es necesario adelantar y fortalecer actividades de socialización de las políticas de tratamiento de datos personales y relación con proveedores, así como soportar los controles de protección de privacidad en aquellos sistemas asociados con el tratamiento de datos personales.

V. RECOMENDACIONES

1. Aplicar la Metodología de Administración para la Gestión de los Riesgos de Seguridad Digital vigente a los procesos de la Entidad.

2. Fortalecer la aplicación de la Metodología de Administración para la Gestión de los Riesgos de Seguridad Digital para cumplir con cada una de las etapas establecidas, enfatizando en la estructuración del diseño de los controles.

3. Fortalecer la ejecución de los controles del anexo A de la norma ISO 27001 que no tuvieron coherencia con lo descrito en la estrategia establecida por la Entidad, de acuerdo con las actividades propuestas.

4. Establecer los mecanismos necesarios para la aprobación y socialización de los documentos del proceso de Gobierno y Seguridad Digital, en especial los relacionados con la continuidad del negocio con el fin de garantizar la prestación de los servicios TIC de la Secretaría de Educación del Distrito.

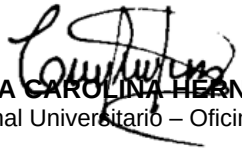
5. Formalizar, publicar y socializar la política de relación con proveedores en su última versión, así como hacer seguimiento al cumplimiento de los lineamientos que allí se establecen por los responsables de

la aplicación de la política (Proveedores y terceros de la SED, Supervisores de Contrato y Equipo de Gobierno y Seguridad Digital).

6. Realizar la gestión pertinente para dar el cierre a la mayor brevedad posible de la acción que se encuentra vencida.

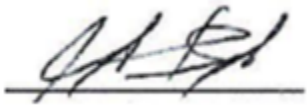
VI. FIRMAS

Informe elaborado por:



ANDREA CAROLINA HERNANDEZ PARDO
Profesional Universitario – Oficina de Control Interno

CAMILO ANDRES CRUZ GONZALEZ
Profesional Universitario – Oficina de Control Interno



JUAN FRANCISCO RODRÍGUEZ FERNÁNDEZ
Profesional Especializado – Oficina de Control Interno

Aprobado por:

OSCAR ANDRES GARCIA PRIETO
Jefe Oficina de Control Interno