Informe Preliminar ☐

Informe Final X

1. NOMBRE DEL INFORME

Auditoria al Sistema de Gestión de Seguridad de la Información SDIS

2. CRITERIOS DE AUDITORÍA

- 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..."
- Ley 1581 de 2012 denominada “Por la cual se dictan disposiciones generales para la protección de datos personales"
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."
- Decreto 607 de diciembre de 2007 "Por el cual se determina el Objeto, la Estructura Organizacional y Funciones de la SDIS"
- Decreto 1078 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
- Decreto 1499 de 2017 – “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 -MIPG- Modelo Integrado de Planeación y Gestión".
- Decreto 591 del 2019 “Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión".
- Modelo de Seguridad y Privacidad de la Información-Norma Técnica Colombiana ISO-27001 Sistema de Gestión de Seguridad de la Información e ISO-27002 guía de buenas prácticas de seguridad de la información.
- Resolución Distrital 305 del 20/10/2008 "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 SDIS 1564 de 2010 “Por la cual se creó el Comité de Seguridad de la Información CSI y define sus funciones”.
- Resolución SDIS 635 de 2017 “Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social”
- Resolución SDIS - 1887 del 12/01/2015 Mediante la cual se deroga la Resolución 1551 de 2007 y se reglamentan las generalidades, operatividad y se dictan otras disposiciones del

sistema de Información de la Secretaría Distrital de Integración Social.
- Circular SDIS 007 del 23/02/2017 sobre Política de seguridad de la información del sitio WEB y protección de datos personales.
- Manuales, Instructivos y Procedimientos Internos.
- Demás normativa vigente relacionada con el objeto y alcance de la auditoría.

3. LÍDER DEL PROCESO, GERENTE DEL PROYECTO, JEFE DE DEPENDENCIA O LÍDER DE SUBSISTEMA AUDITADO

Álvaro Andrés Rueda Zapata – Subdirector de Investigación e Información – Líder de los procesos de Tecnologías de la información y Gestión de soporte y mantenimiento tecnológico.

4. EQUIPO AUDITOR

- Luis Guillermo Patiño Muñoz, Ingeniero de Sistemas - Auditor HSEQ - Auditor Sistema de Gestión de la Seguridad de la Información NTC-ISO/IEC 27001:2013. – Auditor Líder.
- Giovanni Salamanca Ramírez, Auditor HSEQ - Auditor Sistema de Gestión de la Seguridad de la Información NTC-ISO/IEC 27001:2013.
- Francisco José de Jesús Del Vecchio Parra-Auditor HSEQ - Auditor Sistema de Gestión de la Seguridad de la Información NTC-ISO/IEC 27001:2013
- Cesar Mauricio Moreno Castillo - Auditor líder HSEQ - Auditor Interno del Sistema de Gestión de la Seguridad de la Información NTC-ISO/IEC 27001:2013.
- Iris María Córdoba- Auditora HSEQ - Auditor Sistema de Gestión de la Seguridad de la Información NTC-ISO/IEC 27001:2005.
- Sandra Carolina Torres, Auditora HSEQ - Auditora Sistema de Gestión de la Seguridad de la Información NTC-ISO/IEC 27001:2013.

5. OBJETIVO

Verificar el cumplimiento de los requisitos establecidos en el Modelo de Seguridad y Privacidad de la Información-NTC-ISO 27001:2013 y los controles referenciados en el anexo A de la norma, así como, determinar la gestión realizada para el cumplimiento de la documentación asociada a los procesos de Tecnologías de la información y Gestión de soporte y mantenimiento tecnológico.

6. ALCANCE DE LA AUDITORÍA

Cumplimiento de los requisitos establecidos en los capítulos del 4 al 10 de la NTC-ISO 27001 del 2013- Modelo de Seguridad y Privacidad de la Información

Muestra selectiva de los controles establecidos en los 14 dominios del anexo A de la norma y los puntos de control de los Procedimientos objeto de la muestra.

Documentación asociada a los procesos de Tecnologías de la información y Gestión de soporte y mantenimiento tecnológico publicada en el Sistema Integrado de Gestión con corte a 31 de julio de 2019.

7. METODOLOGIA

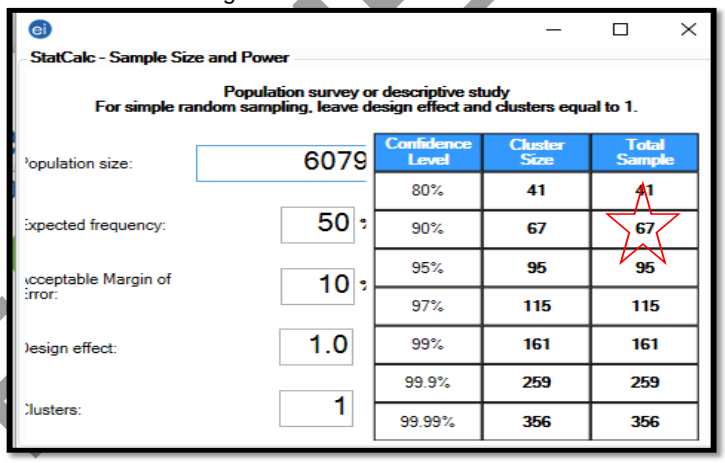
Las actividades desarrolladas por el equipo auditor se resumen metodológicamente en:

7.1 Se realizaron reuniones previas para la planeación de la auditoría con el equipo auditor.
7.2 Elaboración y comunicación del Plan de Auditoría, mediante radicado I2019034319 del 02/08/2019.
7.3 Revisión documental de los Procesos de Tecnologías de la información y Gestión de soporte y mantenimiento tecnológico.

7.4 Determinación de la muestra:

Con el fin de establecer la muestra a evaluar, el equipo auditor solicitó a la Subdirección de Investigación e Información – SII, la base de datos del total de usuarios que tienen acceso a la red interna de la Secretaría Distrital de Integración Social – SDIS (agosto 2019). La SII informó que existen seis mil setenta y nueve (6079) usuarios, con este dato y usando la calculadora estadística StaltCalc del software Epi info, basados en un nivel de confianza del 90% y un margen de error del 10%., se determinó que el tamaño de la muestra a evaluar es de 67 usuarios.

Figura 1 Cálculo de la muestra



Fuente: Resultado calculadora estadística StaltCalc - Epi info.

Una vez definido el tamaño de la muestra, basados en los criterios de muestreo de juicio o discrecional, se incluyeron dependencias que aportan directamente al cumplimiento de los requisitos de la norma técnica ISO 27001 y otras de nivel local, para verificar la implementación de las políticas. Teniendo en cuenta lo anterior fueron priorizadas las siguientes dependencias, con el número de usuarios a evaluar:

- Oficina de Asuntos Disciplinarios: Cinco (5) usuarios.
- Subdirección de Contratación: Cinco (5) usuarios.
- Subdirección de Gestión y Desarrollo de Talento Humano: Cinco (5) usuarios.
- Gestión Documental: Cinco (5) usuarios.

- Apoyo Logístico: Cinco (5) usuarios.
- Subdirección Local de Bosa: Siete (7) usuarios.
- Subdirección local de Engativá: Siete (7) usuarios.
- Subdirección local de Kennedy: Siete (7) usuarios.
- Subdirección local de Mártires: Siete (7) usuarios.
- Subdirección local de Puente Aranda: Siete (7) usuarios.
- Subdirección local de Suba: Siete (7) usuarios.

7.5 Una vez establecida la muestra de la auditoría, el equipo auditor determinó dar alcance al Plan de Auditoría, con el fin de incluir las demás dependencias que potencialmente serían auditadas en el marco de la auditoría, lo cual fue comunicado mediante radicado I2019036852 del 26/08/2019.

7.6 Elaboración de las listas de verificación.
Dado el alcance del Sistema, el equipo auditor determinó crear listas de verificación, para ser aplicadas a los niveles estratégico, táctico y operativo de cada dependencia evaluada.

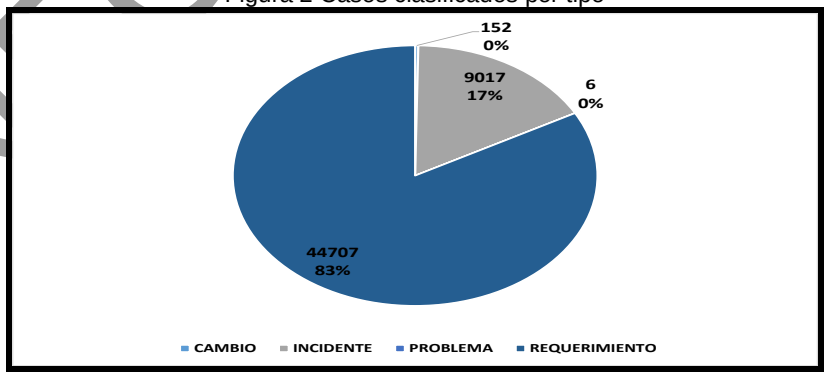
7.7 Aplicación de listas de verificación.
Se aplicaron las listas de verificación por cada nivel, en las dependencias que hicieron parte de la muestra a evaluar (ver numeral 7.4).

7.8 En la mesa técnica del 27/09/2019, se concertó ampliar el desarrollo de la auditoría en 15 días, lo cual fue comunicado mediante radicado I2019042966 del 07/10/2019.

7.9 Se realizó revisión documental y de la información recopilada con los soportes aportados por los responsables.

7.10 De acuerdo con la respuesta suministrada por la SII, frente a que para el periodo comprendido entre enero y agosto de 2019, se recibieron cincuenta y tres mil ochocientos ochenta y dos (53882) casos a través de la mesa de ayuda, se realizó el análisis del total de casos, clasificándolos por tipo, como lo ilustra la siguiente gráfica.

Figura 2 Casos clasificados por tipo



Fuente: Base de datos suministrada por la SII “20190902 Resumen General De Casos SDIS Ene-Ago 2019”

7.11 Se realizaron tres mesas de trabajo los días 11, 27 de septiembre y 29 de octubre de 2019 del equipo auditor junto con el Jefe de la Oficina de Control Interno, para verificar el avance de auditoría y gestionar los riesgos asociados.

7.12 El equipo auditor realizó sesiones de trabajo para analizar los resultados de la revisión documental y los resultados de la auditoria in situ, con el fin de realizar la clasificación de la información.

7.13 Finalmente, el equipo auditor se reunió para analizar la información recolectada para la elaboración del informe preliminar.

Nota: Es responsabilidad de la Subdirección de Investigación e Información y las dependencias donde se aplicaron listas de verificación, el contenido de la información suministrada.

Por parte de la Oficina de Control Interno, la responsabilidad como evaluador independiente, consiste en producir un informe objetivo que contenga las observaciones, si hay lugar a ellas, sobre el acatamiento a las disposiciones legales tanto externas como internas y las recomendaciones que le permitan a la alta dirección tomar decisiones de mejora en la gestión institucional. Conforme lo establecido en el parágrafo del artículo 9 de la Ley 87 de 1993, Control Interno utiliza mecanismos de verificación y evaluación que recogen normas de auditoría generalmente aceptadas y la aplicación de principios como integridad, presentación imparcial, confidencialidad e independencia, los cuales se encuentran sustentados en el enfoque basado en evidencias.

8. DESCRIPCIÓN GENERAL DEL PROCESO, PROYECTO O SUBSISTEMA

La entidad emitió la Resolución 0635 del 12 de abril de 2017 *"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social"*, la cual en su artículo 2 establece como Política General, proteger la información física y lógica que produce, procesa y administra a través de la gestión de riesgos, la implementación de controles de seguridad y el mejoramiento continuo permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información. Ahora bien, aunque el Sistema de Gestión de Seguridad de la Información de la entidad es transversal, se enmarca principalmente en el proceso estratégico de Tecnologías de la Información y el proceso de Soporte Gestión de Soporte y Mantenimiento Tecnológico.

- El proceso de Tecnologías de la Información, Código: CRT-TI-001, Versión: 0, Circular No. 038 - 31/12/2018, tiene como objetivo: "*Identificar, modelar, estructurar, planear, diseñar, adquirir e implementar soluciones estratégicas, misionales y de apoyo, a través de Tecnologías de la Información y las Comunicaciones, acogiendo las mejores prácticas de TIC y la normatividad vigente, con el fin de coadyuvar al cumplimiento de los objetivos institucionales para la optimización de la operación, la consolidación de sistemas de información, la gestión del conocimiento y la toma de decisiones."*

  Este proceso inicia con la identificación de necesidades de tecnologías de la información y las Comunicaciones, continúa con la estructuración, adquisición, implementación y monitoreo de estas, y finaliza con la mejora continua de las tecnologías implementadas.

- El proceso de GESTIÓN DE SOPORTE Y MANTENIMIENTO TECNOLÓGICO, Código: CRT-SMT-001, Versión: 0, Circular No. 038 - 31/12/2018, tiene como objetivo: *"Gestionar la*

continuidad del negocio mediante el soporte y mantenimiento de las Tecnologías de la Información y las Comunicaciones, acogiendo las mejores prácticas de TIC, los lineamientos y directrices internos y la normativa vigente para coadyuvar el cumplimiento de los objetivos institucionales."

El proceso inicia con la recepción de solicitudes de servicios asociados a Tecnologías de la Información y las Comunicaciones, continúa con la gestión de éstas y culmina con el seguimiento y mejoramiento continuo de la provisión de servicios de TIC.

El Sistema de Seguridad de la información, en el marco de los procesos en mención, cuenta con los siguientes documentos asociados en el Mapa de Procesos de la Entidad:

- Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2016-2020.
- PLA-TI-001 versión 0 26/08/2019- Plan de tratamiento del riesgo de seguridad y privacidad de la información.
- PLA-TI-002 versión 0 de 26/08/2019 - Plan de sensibilización, capacitación y comunicación de seguridad y privacidad de la información.
- PLA-TI-003 Versión 0 26/08/2019 - Plan de Seguridad y Privacidad de la Información.
- F-TE-030 Versión 0 de 14/03/2016 - Plan de Contingencia informático.
- MNL-MS-001 versión 0 de 08/03/2018 Manual del Sistema de gestión seguridad de la información – SGSI.
- I-MYSTIC-IF-1 versión 1 de 14/03/2016 Instructivo Informática Forense.
- LIN-MS-001 versión 0 de 08/06/2016 Lineamiento Navegación y uso de aplicaciones web
- LIN-MS-002 versión 0 de 05/03/2018 Lineamiento Administración de contraseñas de las tecnologías de la información.
- LIN-MS-003 versión 0 de 06/06/2018 Lineamiento Control de acceso físico y lógico a las áreas de la subdirección de investigación e información.

9. RESULTADOS AUDITORÍAS ANTERIORES

De acuerdo con la verificación realizada de los planes de mejoramiento internos y externos de las cuatro últimas vigencias, en el Instrumento de Registro y Control de Acciones de Mejora de la Entidad, se evidenció que no existen acciones de mejora, correspondientes a auditorías que tengan como origen o estén relacionadas directamente con el Sistema de Gestión de Seguridad de la Información.

10. HALLAZGOS

En la identificación de los hallazgos se enuncian inicialmente las FORTALEZAS, es decir, aquellas actuaciones relevantes detectadas por el Equipo Auditor en el transcurso de la auditoría, luego se mencionan las OPORTUNIDADES DE MEJORA, situaciones que no implican incumplimientos de requisitos, pero que deben ser tenidas en cuenta para realizar mejoras en los procesos, proyectos o subsistemas o para mitigar posibles riesgos, y por último se plasman las NO CONFORMIDADES que son incumplimientos de los requisitos de acuerdo con los criterios definidos para la auditoría.

Es preciso elaborar un plan de mejoramiento, en el cual se deben incorporar tanto las acciones de mejora en relación con las oportunidades de mejora, las acciones preventivas para atender los riesgos advertidos, como las correcciones y acciones correctivas correspondientes a las no conformidades, para lo cual se debe tener en cuenta el procedimiento definido para tal fin y el correspondiente instrumento de registro, seguimiento y control.

10.1. FORTALEZAS

10.1.1. Durante el ejercicio auditor se evidenció la disposición del personal de la Subdirección de Investigación e Información y de los responsables de la Gestión de la Seguridad de la Información, en las Subdirecciones locales y Nivel Central, para atender las visitas del equipo Auditor.

10.1.2. En el desarrollo de las visitas de auditoría se evidenció que en todos los equipos de los usuarios a quienes se les aplicó la visita tenían acceso a la red y a los servicios asociados, es decir, refleja el cumplimiento del control **A.9.1.2** del anexo A de la ISO 27001, que señala que *"Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente".*

10.1.3 Se evidenció la aplicación de la política de bloqueo de acceso a los equipos de cómputo después de un tiempo determinado.

10.1.4. En desarrollo del ejercicio auditor se evidenció posicionamiento de la mesa de ayuda (Software Aranda), como mecanismo para reportar los requerimientos relacionados con los Sistemas de Información de la Entidad.

10.1.5. Durante el ejercicio auditor, se evidenció que se han implementado por parte de la SII, dos soluciones tecnológicas que permiten hacer uso de los recursos informáticos de manera eficiente; así como, también las medidas para proteger la información como son:

- El almacenamiento de la información institucional basado en la tecnología de disco duros, (SSD- solid-state drive) lo que proporciona un acceso a los datos de manera veloz, y reduce el consumo de corriente eléctrica.

- El servicio en la nube "Azure", para el respaldo de los aplicativos de la Entidad, el cual se encuentra alojado en los Data Centers de Microsoft", cuyo servicio cuenta con las certificaciones en materia de seguridad y protección de datos; fortaleciendo la integridad, confidencialidad y disponibilidad de los datos y las comunicaciones de la Entidad.

10.2. OPORTUNIDADES DE MEJORA

PLANEAR

10.2.1 La Entidad mediante la Resolución 635 de 2017 de la SDIS, determinó que la implementación del Sistema de Gestión de Seguridad de la Información-SGSI, se realice en el marco de la ISO 27001. Teniendo en cuenta lo anterior, en la revisión documental no se evidenció la Declaración de Aplicabilidad, generando riesgo de incumplimiento a lo establecido en el numeral **6.1.3, literal d Tratamiento de riesgos de la seguridad de la información de la**

ISO 27001, que establece que "la organización debe producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A.".

10.2.2 En revisión documental de la Resolución 0635 de 2017 de la SDIS, el equipo auditor evidenció que la relación con proveedores es mencionada en el literal f del artículo 13 el cual establece *"La SDIS a través de la Subdirección de Investigación e Información y la Subdirección de contratación, definirá mecanismos de control, que gobiernen sus relaciones con terceros para asegurar que la información a la que accedan tenga el nivel de protección correspondiente y que éstos cumplan con las políticas y procedimientos de seguridad de la información establecidos*."; sin embargo, al momento de la verificación, no se evidenciaron soportes que den cuenta de la implementación de los controles, mecanismos o procedimientos al respecto. Lo anterior, genera una oportunidad de mejora alineada al control; A.15.1.1 Política de seguridad de la Información para las relaciones con proveedores, que establece *"Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar."*.

10.2.3 En la entrevista del 18/09/2019 con el responsable del plan de continuidad del negocio; se evidenció, que la Entidad cuenta con un borrador del Análisis de Impacto al Negocio -BIA, cuyo objetivo es priorizar las necesidades de recuperación de los servicios y actividades definidas como críticas según los impactos derivados de su interrupción y allí se contemplan actividades propias del SGSI, donde se establecen contratos/convenios relacionados con Servicio de internet, canales MPLS -ETB y servicios de soporte relacionados con sistemas, así como, aplicativos tales como: IOPS, AZ DIGITAL, SIRBE, KACTUS, SIAC, etc., sin embargo; no se evidenció la planeación de simulacros para la ocurrencia de situaciones riesgosas que permitan dar respuesta a la recuperación del sistema (DRP). Lo anterior, podría representar vulnerabilidades en la continuidad del negocio.

10.2.4 En revisión documental de la Resolución 0635 de 2017 de la SDIS, mediante la cual, la entidad adoptó la Política de Seguridad y Privacidad de la Información, se observaron oportunidades de mejora relacionadas con:

- El alcance del manual de la política se refiere al "Subsistema de Seguridad de la información", el cual está derogado.
- La normativa del manual de la política hace referencia a la NTD SIG 001:2011 está derogada.

Lo anterior, podría incumplir con lo establecido en el artículo 16 de la Resolución 0635 de 2017 de la SDIS que señala *"La Política de Seguridad y Privacidad de la Información deberá revisarse y actualizarse cada año*".

10.2.5 De acuerdo con la información suministrada por las Subdirecciones de Gestión y Desarrollo del Talento Humano y Contratación, se evidenció que del total de funcionarios de planta y contratistas (10.163 – ver tabla 1) el 40,1%, correspondiente a 4.084 usuarios, no tienen acceso a la red interna de la SDIS. Lo anterior podría infringir lo establecido en el numeral **7.1 Recursos de la ISO 27001**, que establece "*La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.".*

Tabla 1 Total de funcionarios de planta y contratistas SDIS

Tipo de vinculación	Fecha de corte 31-07-2019
Contratistas	8.272
Servidores de planta	1.891
Total	10.163

Fuente: datos suministrada por las Subdirecciones de GDTH y Contratación

10.2.6 En lo que respecta a la matriz de Inventario de Activos de Información de Tipo Software identificados por las dependencias de la SDIS, con fecha de elaboración del 30/05/2018, la cual se encuentra publicada en "Activos de Información tipo software", del numeral 10.2 *"Registro de Activos de información - Activos de información tipo software"*, del link de transparencia de la SDIS http://www.integracionsocial.gov.co/index.php/transparencia, el equipo auditor identificó algunas diferencias en la información registrada en la matriz, a continuación se señalan algunos ejemplos:

- Los activos de información asociados a la dependencia Subdirección para la Gestión Integral Local, identificados con los numerales 71, 72, 73 y 74, tienen como nombre *"Historias Laborales"* y su descripción corresponde a *"Aplicativo que permite la generación de la historia laboral de los funcionarios de planta de la Entidad mostrando los principales conceptos de nómina.";* así mismo, la mencionada dependencia se registra como dueña de la información. Lo anterior, evidencia una posible incongruencia entre las funciones de la dependencia responsable y el activo identificado.

- Para el caso de la Subdirección de Gestión y Desarrollo del Talento Humano, se registran los activos de información con los numerales 20, 21, 22 y 23, bajo el nombre de "NOMINA WEB - SIAP – BD", con la descripción *"Aplicativo web de nómina que permite la consulta de desprendibles de pago y certificación laboral"*, ahora bien, para la fecha de elaboración (30/05/2018) de la matriz de inventarios de activos de información tipo software, el software de nómina vigente es KACTUS el cual reemplazó al software "NOMINA WEB - SIAP – BD, lo cual presenta una posible inconsistencia en la información publicada.

10.2.7 En la revisión de los documentos publicados en el Mapa de Procesos, se encontraron dentro del "Proceso de Tecnologías de la Información" los siguientes documentos:

- La *"Guía para el Levantamiento de Inventario de Activos de Información a Nivel de Seguridad de la Información"* versión 0 Fecha: Memo INT 13383 – 08/03/2018.
- El documento denominado *"Plan de Contingencia Informático"* versión 1 de Fecha: 14/03/2016.
- El *"Procedimiento Desarrollo y Modificaciones de Software"* versión 1 de Fecha: Circular No. 040 – 29/12/2017.

Dichos documentos están asociados al *"Proceso de Mantenimiento y Soporte de TIC",* el cual ya no existe con ese nombre, en el actual mapa de procesos de la Entidad. Lo cual podría generar una omisión del numeral **7.5.3, e Control de la información documentada de la ISO 27001**, que establece que *"Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable. e) Control de cambios"*, (por ejemplo, control de versión).

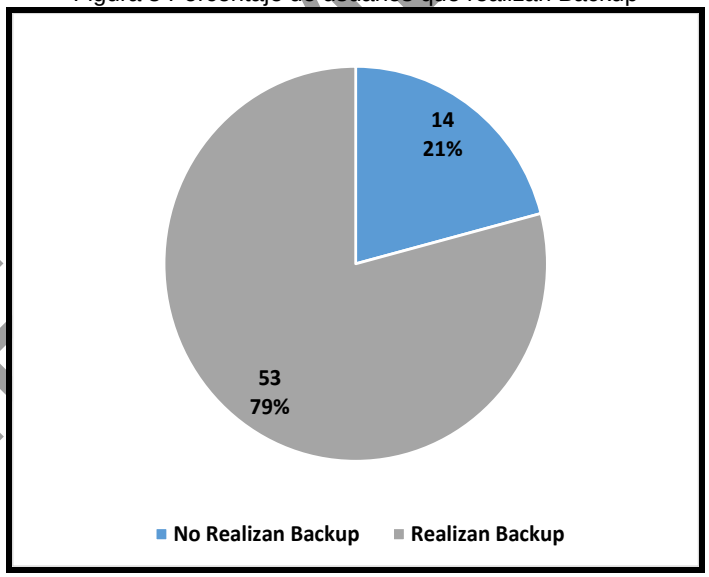
HACER

10.2.8 Consultado el Plan de Seguridad y Privacidad de la Información de la Entidad, publicado en el mapa de procesos con Código: PLA-TI-003 versión 0 de fecha 2019/08/26, se establecieron tareas, como "*Socializar Guía de Activos de Información"* y *"Generar Nueva Versión de la Política de Seguridad y Privacidad de la Información de la Entidad",* las cuales tienen como fecha para ejecución, julio de 2019; no obstante en la entrevista con el proceso no fueron presentadas evidencias de su cumplimiento. Lo que podría generar una posible inobservancia al plan de implementación.

10.2.9 En la visita realizada para verificar el respaldo de los servicios en la nube de "Azure", se evidenció que en el momento de la visita 2019/09/13 el aplicativo misional SIRBE, aún no contaba con la copia de respaldo en el servicio mencionado. Lo que podría generar un posible riesgo de pérdida de la información.

10.2.10 De los 67 usuarios entrevistados, 14 de ellos (21%) no realizan Backup o copias de respaldo de la información. Lo anterior podría generar una desatención al objetivo del control **A.12.3.1. Respaldo de la información de la 27001**, que reza *"Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.".* Así como, lo establecido en el artículo 5 literal f de la Resolución 635 de 2017 de la SDIS. Lo que podría causar la pérdida de datos de información importantes para la entidad.

Figura 3 Porcentaje de usuarios que realizan Backup



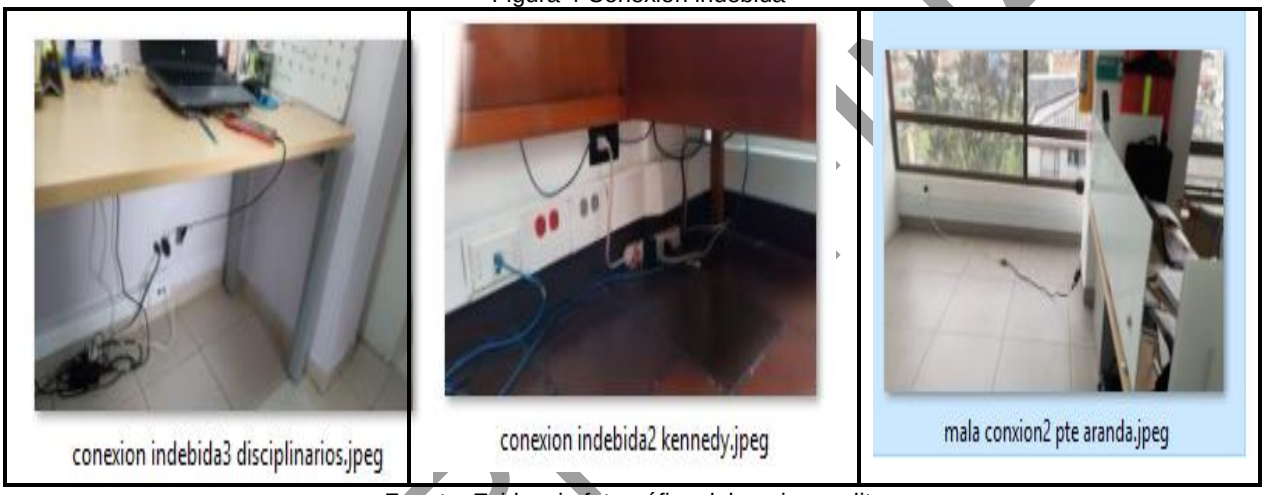
Fuente: Resultados análisis listas de verificación

10.2.11 En revisión de los documentos publicados en link de transparencia de la SDIS http://www.integracionsocial.gov.co/index.php/transparencia, numeral 10.2 *"Registro de Activos de información - Activos de información tipo software"*, se evidenció que se encuentran publicados en "Registro de Activos de Información", los cuadros de caracterización documental, por cada dependencia de la SDIS, los cuales no se encuentran alineados a los procesos del

actual Mapa de Procesos de la Entidad, así mismo, éstos presentan como fecha de actualización el 14 de junio de 2018. Lo anterior podría generar una inobservancia al **artículo 9 de la Resolución 0635 de 2017** de la SDIS que señala *"Los dueños de la información deben propender para que los custodios mantengan actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez por año".*

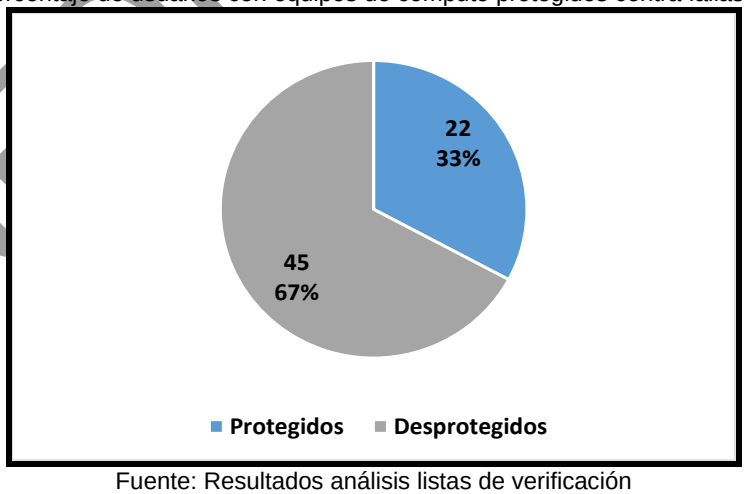
10.2.12 En la tabulación de las listas de verificación aplicadas, se evidenció en el 67 % de los usuarios (45 de 67), que los equipos de cómputo no están protegidos contra fallas de energía; Lo cual podría establecer una inobservancia del objetivo del control **A.11.2.2 Servicios de suministro de la ISO 27001**, que reza *"Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro."*

Figura 4 Conexión indebida



Fuente: Evidencia fotográfica del equipo auditor

Figura 5 Porcentaje de usuarios con equipos de cómputo protegidos contra fallas de energía



Fuente: Resultados análisis listas de verificación

VERIFICAR

10.2.13 En revisión documental, no se evidenciaron actas de reuniones del Comité de Seguridad de la Información, correspondiente al periodo comprendido entre 01/01/2018 y el 25/02/2019 fecha en que estaba vigente la Resolución 1075 de 2017.

Así mismo, en lo que corresponde al periodo del 26/02/2019 al 31/07/2019, no fueron entregados al equipo auditor documentos que den cuenta de las reuniones realizadas por el Comité Institucional de Gestión y desempeño de acuerdo con la Resolución 355 de 2019, donde traten temas de seguridad de la información. Lo cual podría generar dificultades en el apoyo por parte de la alta dirección para soportar la administración y desarrollo de iniciativas sobre seguridad de la información y para el mantenimiento de la política de privacidad y seguridad de la información.

10.3. NO CONFORMIDADES

10.3.1 En visitas al piso 18 de Nivel Central, a la Subdirección de Contratación, SLIS Kennedy, SLIS Puente Aranda y SLIS Engativá, se evidenció que se encuentran activos de información (Equipos y documentos) que no cuentan con las debidas protecciones físicas y de seguridad requeridas tal como se evidencia en las figuras 3 y 4. Dado que mediante la Resolución 635 de 2017 de la SDIS, la entidad determinó que la implementación del Sistema de Gestión de Seguridad de la Información-SGSI, se realice en el marco de la ISO 27001, se incumple con el objetivo de control **A.11.1 Áreas seguras de la ISO 27001** que señala que se debe "Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización (..).", así como lo establecido en el artículo 12 de la Resolución 635 de 2017 de la SDIS que establece *"Uso aceptable de los activos: Los recursos tecnológicos al igual que los archivos, carpetas, base de datos, aplicaciones y documentos, son activos de información que pertenecen a la SDIS, por lo cual su uso es exclusivamente institucional y es responsabilidad de aquel a quien se asigne o corresponda su uso, el propender por su confidencialidad, integridad, disponibilidad, privacidad y buen uso"* .Lo anterior tiene como consecuencia el probable daño físico e indisponibilidad de los servicios que se brindan a través de la red y la exposición de la información documental y el soporte de las transacciones de la Entidad.

Figura 6 Activos sin protección física

Fuente: Evidencia fotográfica del equipo auditor

Figura 7 Activos sin protección física

Fuente: Evidencia fotográfica del equipo auditor

10.3.2 El 24 % de los usuarios a los que se le aplicó la lista de verificación, correspondiente a 16 personas de las 67 entrevistadas, no conocen la política del Sistema de Gestión de la Seguridad de la Información de la Entidad. Así mismo, en revisión documental no se evidenciaron soportes de la divulgación de la política de seguridad y privacidad de la información, por parte de la Subdirección de Gestión y Desarrollo de Talento Humano, ni de la Subdirección de Contratación. Incumpliendo el artículo 7 de la Resolución 0635 de 2017 de la SDIS, el cual establece que "La SDIS a través de la Subdirección de Gestión y Desarrollo de Talento Humano y la Subdirección de Contratación es la responsable de divulgar la Política de Seguridad y Privacidad de la Información a todos los funcionarios o contratistas que se vinculen a la entidad".

10.3.3 En revisión de los documentos asociados a los procesos "Tecnologías de la Información" y "Gestión de Soporte y Mantenimiento Tecnológico" publicados en el Mapa de Procesos de la Entidad, se evidenció que no se cuenta con un procedimiento, guía o protocolo para la revisión por la Dirección del Sistema de Gestión de Seguridad de la Información, así como también en las carpetas compartidas por la SII, mediante One Drive, los registros no dan cuenta que en la Revisión por la Dirección se hayan desarrollado las temáticas solicitadas en los literales a, b, c, d, f del numeral **9.3 Revisión Por La Dirección de la ISO 27001**, que establece que *"La alta dirección debe revisar el Sistema de Gestión de la Seguridad de la Información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas".*

11. RIESGOS

11.1. En la revisión de los procesos de Tecnologías de la Información y Gestión de Soporte y Mantenimiento Tecnológico, se identificó que sus objetivos, productos, alcance y puntos de control son diferentes, ahora bien, el equipo auditor evidenció que las Matrices de Riesgos publicadas para los dos procesos contienen la misma información, y cuyos riesgos deberían estar alineados de acuerdo a su objetivo y alcance descrito en la caracterización de cada uno de los procesos, tal como se aprecia en la siguiente tabla:

Tabla 2 Riesgos Asociados a los Procesos de Tecnologías de la Información y Gestión de Soporte y Mantenimiento Tecnológico

Proceso Tecnologías de la información			**Proceso Gestión de soporte y mantenimiento tecnológico**		
Cod.	**Causa**	**Riesgo**	**Cod.**	**Causa**	**Riesgo**
RTIC-20	Suministro eléctrico inestable Desastres ocasionados por el hombre Inadecuado sistema de prevención de atención de desastres y mantenimiento del suministro	Indisponibilidad parcial o total de los sistemas de información misionales de la SDIS	RTIC-20	Suministro eléctrico inestable Desastres ocasionados por el hombre Inadecuado sistema de prevención de atención de desastres y mantenimiento del suministro	Indisponibilidad parcial o total de los sistemas de información misionales de la SDIS
RTIC-21	Inadecuada clasificación de activos Protección inadecuada de bases de datos (roles, responsabilidades) Uso de software malicioso Falta de esquemas de alta disponibilidad (respaldo) Uso de dispositivos móviles Políticas de almacenamiento físico inapropiado	Indisponibilidad parcial o total de la información contenida en las bases de datos misionales de la SDIS	RTIC-21	Inadecuada clasificación de activos Protección inadecuada de bases de datos (roles, responsabilidades) Uso de software malicioso Falta de esquemas de alta disponibilidad (respaldo) Uso de dispositivos móviles Políticas de almacenamiento físico inapropiado	Indisponibilidad parcial o total de la información contenida en las bases de datos misionales de la SDIS

RTIC-23	Falta de controles en las herramientas de ingreso de la información Error humano en la consecución o captura del dato Inestabilidad de los canales de comunicaciones Múltiples fuentes de información Fallos en la infraestructura que soporta la operación	Deficiencia en la calidad y completitud del dato primario (dirección), como insumo único para la ubicación espacial o georeferenciación requerida	RTIC-23	Falta de controles en las herramientas de ingreso de la información Error humano en la consecución o captura del dato Inestabilidad de los canales de comunicaciones Múltiples fuentes de información Fallos en la infraestructura que soporta la operación	Deficiencia en la calidad y completitud del dato primario (dirección), como insumo único para la ubicación espacial o georeferenciación requerida
RTIC-24	Inadecuada o inexistente documentación del código fuente Falta de control sobre los tiempos comprometidos Errores en la contratación del personal Deficiencia en el desarrollo del plan pruebas Deficiencia en el levantamiento de requerimiento solicitado. Falta de conocimiento y aprobación del requerimiento por parte de todos los involucrados en dicho proceso.	Retrasos en los desarrollos solicitados al Equipo de Factoría de Software	RTIC-24	Inadecuada o inexistente documentación del código fuente Falta de control sobre los tiempos comprometidos Errores en la contratación del personal Deficiencia en el desarrollo del plan pruebas Deficiencia en el levantamiento de requerimiento solicitado. Falta de conocimiento y aprobación del requerimiento por parte de todos los involucrados en dicho proceso.	Retrasos en los desarrollos solicitados al Equipo de Factoría de Software
RTIC-25	Falta supervisión en la elaboración de la documentación funcional y técnica. No incluir actividad de documentación el cronograma de trabajo del desarrollo. Falta disponibilidad de tiempo para la elaboración de documentación. Rotación del personal calificado para las actividades de desarrollo.	Falta de documentación técnica y funcional de los aplicativos	RTIC-25	Falta supervisión en la elaboración de la documentación funcional y técnica. No incluir actividad de documentación el cronograma de trabajo del desarrollo. Falta disponibilidad de tiempo para la elaboración de documentación. Rotación del personal calificado para las actividades de desarrollo.	Falta de documentación técnica y funcional de los aplicativos
RTIC-29	Ausencia de criterios claros para la selección y asignación de los supervisores a los contratos de Tecnologías de la Información -TI.	Negligencia en la supervisión de los contratos de Tecnologías de la Información -TI	RTIC-29	Ausencia de criterios claros para la selección y asignación de los supervisores a los contratos de Tecnologías de la Información -TI.	Negligencia en la supervisión de los contratos de Tecnologías de la Información -TI

Fuente: Matrices de identificación, clasificación y valoración de riesgos de los Procesos de Tecnologías de la Información y Gestión de Soporte y Mantenimiento Tecnológico

11.2. En el desarrollo del ejercicio auditor, se evidenció que los controles definidos en la "matriz de identificación, clasificación y valoración de riesgos" con código F-MC-AR-001 en el campo controles del documento, no se encuentran alineados con las seis (6) variables definidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del departamento administrativo de la función pública, los cuales se relacionan a continuación:

1. Debe tener definido el responsable de llevar a cabo la actividad de control,
2. Debe tener una periodicidad definida para su ejecución,
3. Debe indicar cuál es el propósito del control,
4. Debe establecer el cómo se realiza la actividad de control,
5. Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control y
6. Debe dejar evidencia de la ejecución del control.".

11.3. Se evidenció la desactualización en el Mapa de Procesos de las matrices de riesgos de los procesos de "Tecnologías de la información" y de "Gestión de soporte y mantenimiento tecnológico", dado que está publicada la versión 2 del 31/12/2015.

Nota: Es importante indicar que la Política de Administración de Riesgos de la Entidad (vigente), fue oficializada bajo Memo I2019022553 del 29/04/2019 (código LIN-GS-001), la misma estableció en su numeral 10 "*Los riesgos en la Secretaría Distrital de Integración Social se categorizan por procesos, entendiendo que, si en el marco de los planes, programas o proyectos se identifican riesgos, estos se deben enmarcar dentro de los procesos institucionales."*

12. CONCLUSIONES

- La Entidad viene realizando las acciones conducentes para dar cumplimiento con los requisitos del Modelo de Seguridad y Privacidad de la Información y la NTC-ISO 27001:2013; no obstante, se identificaron oportunidades de mejora y no conformidades.

- La Entidad presenta oportunidades de mejora respecto del cumplimiento del Anexo A Controles de la NTC-ISO 27001:2013

- La Entidad cuenta con matrices de riesgos iguales para los procesos de Tecnologías de la Información y de Gestión de Soporte y Mantenimiento Tecnológico, lo cual no permite garantizar que la gestión del riesgo sea utilizada como una herramienta gerencial de apoyo para el cumplimiento de objetivos del Sistema de Gestión de Seguridad de la Información.

Nota: Las auditorías se realizan con técnicas de muestreo, lo que significa que no todas las no conformidades han sido detectadas, ni que aquellas partes no revisadas no presenten no conformidades.

13. RECOMENDACIONES

- Se recomienda a la Entidad tomar las acciones pertinentes para garantizar el cierre de los hallazgos identificados en la auditoría.

- Dar cumplimiento estricto a la normativa vigente asociada a la Gestión de Seguridad de la Información en la Entidad.

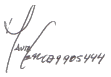
- Intensificar los esfuerzos para realizar la identificación de riesgos de los procesos de Tecnologías de la información y de Gestión de soporte y mantenimiento tecnológico, y por ende la actualización de las matrices de riesgos de los procesos objeto de la auditoria. Así como, alinear los controles de los riesgos con los lineamientos emitidos por Departamento Administrativo de la Función Pública-DAFP.

- Continuar fortaleciendo el plan de continuidad del negocio, realizando pruebas que contemplen escenarios de indisponibilidad del servicio, con el fin de contar con una herramienta que responda a los eventos adversos o catastróficos.

- Dar continuidad a la implementación del Modelo de Seguridad y Privacidad de la Información a nivel Institucional como mecanismo de aseguramiento de la Confidencialidad, Integridad y Disponibilidad de la información.

- Realizar de manera oportuna el seguimiento, monitoreo y evaluación al Sistema de Gestión de Seguridad de la Información de la Entidad.

- Se recomienda analizar la viabilidad de definir mecanismos para garantizar la transferencia del conocimiento en lo relacionado con tecnología en las actividades inherentes a la confidencialidad, integridad y disponibilidad de la información para garantizar la continuidad del negocio y gestión ante la posible pérdida de los activos de información críticos.

EQUIPO AUDITOR	Firma(s):
Luis Guillermo Patiño Muñoz.	
Giovanni Salamanca Ramírez	
Francisco José de Jesús Del Vecchio Parra	
Cesar Mauricio Moreno Castillo	
Iris María Córdoba Dávila	
Sandra Carolina Torres Sáez	

JEFE OFICINA CONTROL INTERNO	Firma:
Yolman Julián Sáenz Santamaría	

FECHA DE ENTREGA	
Informe Preliminar ☐	22-11-2019
Informe Final X	