Proceso:	**Dirección Administrativa - Sistemas y Seguridad de la Información**
Líder del proceso/Jefe de dependencia:	Dra. Nubia Stella Suárez Sotelo – Directora Administrativa
Objeto:	Verificar la eficacia del proceso Sistemas y Seguridad de la Información, de acuerdo con los requerimientos del Modelo Integrado de Planeación y Gestión – MIPG y la normatividad aplicable; con el objetivo de establecer oportunidades de mejora, que contribuyan al cumplimiento de los objetivos institucionales y a fortalecer el Sistema de Control Interno.
Alcance:	Cubre el proceso de Sistemas y Seguridad de la Información a través de la evaluación de los procedimientos de: SSI-PR001 Administración y actualización de la red y servidores, SSI-PR003 Atención de soporte tecnológico, SSI-PR005 Plan de necesidades de contratación y seguimiento a los contratos de tecnología, SSI-PR009 Acceso físico a las instalaciones e ingreso de equipos portátiles, SSI-PR010 Acceso lógico, SSI-PR011 Gestión de activos. **Periodo a auditar**: Agosto de 2022 a Julio de 2023.
Criterios:	- Constitución Política de Colombia. - Ley 1952 de 2019 "*Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario*". - Ley 909 de 2004 "*Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones*" y sus reglamentarios. - Ley 80 de 1993 "*Por la cual se expide el Estatuto General de Contratación de la Administración Pública*" y sus reglamentarias. - 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*". - Ley 1712 de 2014 "*Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública Nacional*". - Ley 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales*", Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. - Ley 1266 de 2008 "*Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*".

	- 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 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*" - Decreto 338 de 2022 "*Por el cual se adiciona el Título 21 a la Parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones*". - Decreto 1083 de 2015 "*Por medio del cual se expide el Decreto Único reglamentario del sector de Función Pública*" (Adiciones y modificaciones). - Decreto 338 de 2019, "*Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción*". - 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 1519 de 2020 "*Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos*". - Resolución 305 de 2008, Secretaría General Alcaldía Mayor de Bogotá, D.C. - Comisión Distrital de Sistemas – CDS "*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, Secretaria General Alcaldía Mayor de Bogotá D.C. "*Por medio de la cual se modifica la Resolución 305 de 2008 de la CDS*". - Resolución 720 de 2013 "*Por la cual se aprueba el Manual de Procesos y Procedimientos del Concejo de Bogotá D.C.*" - Resolución 634 de 2014 "*Por la cual se adopta el Organigrama del Concejo de Bogotá D.C."* - Resolución 635 de 2014 "*Por la cual se adopta el Normograma del Concejo de Bogotá D.C.*"

	- Resolución 1007 de 2015 "*Por medio del cual se modifica la resolución No. 1323 del 2012 "Por la cual establece el Mapa de Procesos del Sistema Integrado de Gestión del Concejo de Bogotá, D.C.*". - Resolución 0571 de 2015 "*Por el cual se deroga la resolución No. 1086 del 2012, y se implementa el plan de contingencias para los sistemas de información del concejo de Bogotá, D.C.*" - Resolución 514 de 2015 "*Por la cual se actualiza el Manual especifico de Funciones y Competencias Laborales de los empleos de planta de personal del Concejo de Bogotá D.C.*" y sus modificatorias. - Resolución 388 de 2019 "*Por medio de la cual se adopta el MIPG, Crea el Comité Institucional de Gestión y Desempeño*". - Resolución 428 de 2021 "*Por medio de la cual se modifica la Resolución 388 de 2019*". - Resolución 343 de 2020 "*Por medio de la cual se adopta la Plataforma Estratégica y el Plan de Acción Cuatrienal del Concejo de Bogotá, D.C. para el periodo 2020- 2023*". - Resolución 0317 de 2022 "*Por medio de la cual se modifica la Resolución 343 de 2020*". - Resolución 0064 de 2023 "*Por medio de la cual se adopta el Plan de Acción para la vigencia 2023*". - Guía para la administración del riesgo y el diseño de controles en las entidades públicas DAFP 2022 v5. - Guía para la construcción y análisis de indicadores de gestión DAFP. - Directiva 2 de 2002 de la Presidencia de la República, Asunto: Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software). - Norma Técnica Colombiana NTC 5854 de 2011 "Accesibilidad a páginas Web". - Norma ISO 27001 de 2013 "Sistemas de Gestión de Seguridad de la Información". - CONPES 3670 de 2010 "Lineamientos de política para la continuidad de los Programas de Acceso y Servicio Universal a las Tecnologías de la Información y Comunicación". - CONPES 3701 de 2011 "Lineamientos de política para ciberseguridad y ciberdefensa". - CONPES 3854 de 2016 "Política Nacional de Seguridad Digital". - Política de Gobierno Digital. Demás Normas que les apliquen.
Equipo Auditor:	Carlos Andrés Padilla Pinto. José Gabriel Parra Pirazan.
Auditados:	Nubia Stella Suárez Sotelo – Directora Administrativa. William Darío Ávila Díaz. Francisco Javier Bernal García.

	Luis Argenio Mariño Roa. Diego Andrés Lemus Rodríguez. Francisco Alfonso Naranjo Madero. Equipo de trabajo y contratistas del Proceso.	
Metodología:	De acuerdo al plan de auditoria, se remitió al proceso auditado un cuestionario de preguntas mediante Memorando 2023IE12626, el cual se organizó por grupos con el fin de que el proceso realizara la consolidación y envío de respuestas de acuerdo a un cronograma, lo cual facilitó el análisis de las mismas por parte de los auditores. Así mismo, se realizó la revisión de la información del proceso ubicada en las unidades de red, la intranet y la página web de la corporación y, se realizaron entrevistas con los profesionales y funcionarios en la Oficina del Proceso SSI.	
Fechas de Ejecución de la Auditoría:	Desde (día/mes/año):	24 agosto de 2023
	Hasta (día/mes/año):	31 de octubre de 2023
Reunión de Cierre:	(día/mes/año):	10 de octubre de 2023

I. PROCESO SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN – TEMAS GENERALES

1. CONFORMIDADES

Se realiza el análisis de conformidades, según cuestionario remitido el 29 de agosto de 2023.

1.1. En respuesta y cumplimiento a la caracterización SSI-CA-001 versión 3, en los referente a "Elaborar el plan para la implementación del modelo de privacidad de la información", evidenciando que para la vigencia 2023 el proceso elaboró y publicó el Plan en la ruta https://concejodebogota.gov.co/4-3-otros-planes-institucionales/cbogota/2022-07-26/114625.php, lo anterior de acuerdo a lo solicitado en el cuestionario de auditoria.

1.2. De acuerdo con la información reportada, se da conformidad a las actividades 1, 3 y 4 del plan para la implementación del Modelo de Privacidad y Seguridad de la Información, en el que se evidenciaron 2 autodiagnósticos con fechas de corte 31/12/2022 y 30/06/2023. Con relación al seguimiento a los planes de mejora del SGSI, el proceso ha venido presentando avances a los planes de mejora suscritos, sin embargo, se recomienda aunar esfuerzos para dar cierre a las no conformidades que continúan abiertas. En el segundo semestre del año 2022 se evidenciaron 3 socializaciones en temas de seguridad de la información.

1.3. Se da conformidad a lo solicitado, frente a la elaboración del plan de tratamiento de riesgos de seguridad de la información de acuerdo con la metodología adoptada por la entidad, en el cual se pudo evidenciar la publicación de los riesgos de gestión del proceso Sistemas y Seguridad de la información en el formato GMC-FO-003 versión 01, en la ruta de las unidades de red U:\Administración de Riesgos\2023\ 12_MAPA DE RIESGOS DE GESTIÓN SSI 2023.xlsx y en la página web de la Corporación botón Transparencia https://concejodebogota.gov.co/4-3-otros-planes-institucionales/cbogota/2022-07-26/114625.php.

1.4. Se evidenció que el proceso SSI realizó estudios de necesidades para la adquisición de nuevas tecnologías para la entidad, actividad soportada mediante memorando 2023IE951 remitido a las diferentes dependencias de la Corporación el día 23 de enero de 2023, con el propósito de conocer las necesidades de tecnología; el proceso consolidó la información y analizó la pertinencia de los requerimiento, con el fin de incluirlos o no en futuros procesos de contratación.

1.5. De acuerdo con la información reportada, se observa que el proceso publicó para las vigencias 2022 y 2023 los indicadores de gestión en las unidades de red U:\Indicadores de Gestion\Año 2022 y U:\Indicadores de Gestion\Año 2023 12. Sistemas_Seguridad_Informacion.xlsx, documentos en los que se evidencia 3 indicadores: Encuestas de satisfacción realizadas, soportes de la mesa de ayuda realizados y Backup realizados, los cuales presentan una verificación semestral, por lo tanto, se da conformidad a lo descrito en la caracterización SSI-CA-001 versión 3 y lo solicitado en el cuestionario de auditoria.

1.6. De acuerdo con la información reportada, se observó que el proceso SSI a través del contrato de mesa de servicios No. 220391 de 2022 con SELCOMP INGENIERIA SAS, realizó 175 mantenimientos preventivos correspondientes a 143 computadores de escritorio, 29 computadores portátiles y 3 impresoras, luego de verificados los soportes se evidenciaron 175 “Formatos de mantenimiento preventivo y toma de datos” realizados entre el 20 de octubre y el 28 de noviembre de 2022. El contrato actual de mesa de servicios No. 230427 con SELCOMP INGENIERIA SAS, está realizando los mantenimientos preventivos, los cuales empezaron el 18 de septiembre.

1.7. De acuerdo a lo reportado, sobre la descripción del control para el riesgo de gestión No. 1 relacionado con la transferencia de conocimiento a los funcionarios en el manejo de las herramientas; se evidenciaron videos, grabaciones y actas de asistencia a capacitaciones o sesiones de transferencia de conocimiento sobre los bienes o servicios adquiridos mediante los contratos 220885 cámaras fotográficas, 220581 Gestor de Contenido Prontus Página Web y Janus, 220860 Software Streaming, 220529 Adobe Corel Draw, 220887 Sistema de Conferencia y Debate, 220785 Adquisición de Escáner, 220837 procesos de ITIL y 220774 Impresoras de Etiquetas, por lo anterior, se da conformidad a lo descrito en el control y lo solicitado en el cuestionario de auditoria.

1.8. Se da conformidad a la pregunta 11 relacionada con la elaboración de fichas técnicas y solicitudes de contratación, se verificaron los soportes de correos electrónicos enviados desde la Dirección Administrativa a la cuenta gestion.pagos@concejobogota.gov.co, los cuales luego de revisarlos y filtrarlos, se observaron 54 Fichas técnicas y solicitudes de contratación.

1.9. Con relación a los riegos de corrupción y la descripción del control para el riego No. 9, se verifico la información reportada por el proceso, en la cual se constató la manera en la que el software de administración y monitoreo realiza diariamente las copias de seguridad de la información y como el profesional asignado realiza el seguimiento, los reportes diarios son verificados y, en caso de existir algún error, el funcionario vuelve a lanzar el Backup fallido; la correlación de eventos generados por el sistema son registrados diariamente en el Formato SSI-PR002-FO1.

1.10. Luego de revisada y analizada la información de algunos contratos seleccionados de manera aleatoria, relacionada con los acuerdo de confidencialidad firmados entre la

Corporación y entidades externas, se pudo confirmar que los mismos fueron suscritos, por lo tanto, se da conformidad a lo solicitado en la pregunta No. 55 del cuestionario de auditoria.

2. NO CONFORMIDADES

2.1. Se evidencio que el proceso no dio cumplimiento a la Actividad No. 2 del Plan del Modelo de Seguridad y Privacidad y Seguridad de la Información, relacionado con el Manual de políticas de Seguridad de la Información revisado y actualizado para la vigencia 2022, si bien en cierto, en la ruta Q:\12_SSI\Auditorias internas\Auditoria 2023\Rta Pregunta 2\2.2 Evidencia Revisión Manual, se observan 2 documentos: "*Borrador Resolución Política Seguridad Concejo Bogota.docx"* y "*Manual de Politicas Especificas.docx*", este último archivo contiene el formato SSI-MA-001 Manual de Políticas de Seguridad de la Información, con algunas revisiones y comentarios de fecha 12 y 13 de octubre de 2022, elaboradas por Khaanko Norberto Ruiz, es un documento en proyecto sin solicitud de revisión metodológica para posterior validación y aprobación en el CIGD. El Manual de Políticas que está vigente y publicado en las unidades de red U:\Manual de Procesos y Procedimientos\12-Sistemas y Seguridad de la Informacion\2_Manuales\ SSI-MA-001_Manual_Politicas_Seguridad_Información V04.pdf, tiene fecha de control de cambios 29 de junio de 2021, adicionalmente, se observó que este documento no está firmado por 2 funcionarios que apoyaron la elaboración o actualización.

Lo anterior, producto de debilidades en la revisión y actualización documental de los procedimientos, manuales, guías y formatos del proceso SSI. Así como, la disponibilidad de un responsable de seguridad de la información de manera permanente. Por lo tanto, la Corporación no cuenta con un Manual de Políticas de Seguridad de la Información actualizado, no es un documento confiable para la gestión de la seguridad de la información en la entidad.

Hecho que infringe lo descrito en el numeral 2 del Manual de Roles y Responsabilidades de Seguridad de la Información Código SSI-MA003, relacionado con las funciones del Responsable de Seguridad de la Información, entre otras funciones: "*Garantizar que exista la documentación relacionada con el SGSI, considerando control de cambios de versión, aseguramiento, clasificación y disponibilidad*", y numeral 4.1 Roles y responsabilidades del sistema de gestión de seguridad de la información, del mismo Manual de Políticas de Seguridad de la Información Código SSI-MA-001 "*Responsable de Seguridad de la Información: Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Equipo Técnico de Seguridad de la Información, realizando la implementación y seguimiento de estos*".

De igual manera, incumple lo señalado en la Resolución 500 de 2021 MINTIC, articulo 3: Lineamientos generales. "*(…) Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. (….) Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital*".

Incumple lo definido en la Ley 87 de 1993, articulo 2. Objetivos del Sistema de Control Interno, literal a. "*Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que lo afecten".* Literal e. *"Asegurar la oportunidad y confiabilidad de la información y de sus registros"*.

OBJECIONES PRESENTADAS POR EL PROCESO

Memorando 2023IE14832 del 20 de octubre d e2023, “Se precisa que la Política y el Manual de Políticas se presentarán en la próxima reunión del Equipo Técnico de Seguridad de la Información, para su aprobación y trámite ante el Comité Institucional de Gestión y Desempeño – CIGD, se anexa borrador de los documentos actualizados.

En cuanto a la disponibilidad de un responsable de seguridad de la información de manera permanente, el proceso SSI ha manifestado en diferentes espacios que para esta actividad se debe contar con un recurso humano permanente, pero dado que esto implica una restructuración de la planta de personal de la Corporación, todos los años solicita en el plan de adquisiciones la contratación de un profesional con el perfil requerido, sin embargo no siempre se ha contado con la disponibilidad de recursos para adelantar el proceso contractual.”

Evidencia:

Los documentos pueden ser consultados en la ruta
Q:\12_SSI\Auditorias internas\Evidencias PM 2023\2.1

RESPUESTA A LA OBJECIÓN POR PARTE DE LA OFICINA DE CONTROL INTERNO

Analizada la respuesta y consultadas las evidencias, se comprueba que el Proceso Sistemas y Seguridad de la Información no dio cumplimiento a la Actividad No. 2 del Plan del Modelo de Seguridad y Privacidad y Seguridad de la Información, relacionado con el Manual de Políticas de Seguridad de la Información revisado y actualizado para la vigencia 2022, esta actividad tenia fecha cumplimiento diciembre de 2022.

Por lo tanto, no se acepta la réplica a esta No Conformidad, se ratifica y se debe formular el respectivo plan de mejoramiento.

Calificación del riesgo de la No conformidad

Probabilidad	Muy Baja (20%)	**Impacto**	Moderado (60%)	**Calificación del Riesgo**	Moderado

2.2. Se observó que el Manual de Roles y Responsabilidades de Seguridad de la Información Código SSI-MA003 Versión 01, esta desactualizado, toda vez que hace referencia a comités técnicos que fueron asumidos por el Comité Institucional de Gestión y Desempeño con la expedición de la Resolución 388 de 2019 “Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, se crea el Comité Institucional de Gestión y Desempeño y se dictan otras disposiciones”, modificada por la Resolución 428 de 2021. Se debe tener en cuenta la guía de la Dirección de Gobierno Digital versión 4 del 28/10/2021.

Situación que es producto de falencias en la revisión y actualización documental del proceso SSI. Por lo tanto, la entidad no posee un documento actualizado que facilite a los servidores identificar de manera clara los roles y responsabilidades de en materia de seguridad de la información.

Incumple lo definido en la ley 87 de 1993, articulo 2. Objetivos del Sistema de Control Interno, literal b. “*Garantizar la eficacia, la eficiencia y economía en todas las operaciones promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para*

el logro de la misión institucional". Literal e. *"Asegurar la oportunidad y confiabilidad de la información y de sus registros"*. Incumple lo dispuesto en el Procedimiento de control de documentos del SIG, Código GMC-PR-004, Versión 10, Numeral 5.1 "*REALIZAR LA CREACIÓN O MODIFICACIÓN O ELIMINACIÓN DEL DOCUMENTO. Realiza la propuesta de actualización documental junto con los servidores y colaboradores responsables de desarrollar las actividades, conforme a las necesidades del proceso y remite propuesta junto con el formato "Solicitud actualización documental" GMC-FO-001 diligenciado, al correo electrónico planeacion@concejobogota.gov.co.",* responsables: Líder e integrantes del proceso.

OBJECIONES PRESENTADAS POR EL PROCESO

Ante la No Conformidad 2.2, y de acuerdo al memorando 2023IE14832 del 20 de octubre, el proceso no presentó objeciones; por lo tanto, se confirma la No Conformidad y se debe formular el respectivo plan de mejoramiento.

Calificación del riesgo de la No conformidad

Probabilidad	Muy Baja (20%)	**Impacto**	Menor (40%)	**Calificación del Riesgo**	Bajo

2.3. Luego de verificados los soportes y, analizadas las respuestas al cuestionario de auditoria, se evidencio que el Equipo Técnico de Seguridad de la Información no se ha reunido en lo que va corrido del año. Situación generada por debilidades en la coordinación del líder del Equipo Técnico para definir los esquemas de operación y la periodicidad con las que se adelantan las reuniones.

Como consecuencia, se presenta atraso en los temas relacionados principalmente con las Políticas de Gobierno y Seguridad Digital, los cuales deben ser presentados y abordados en el comité CIGD.

Lo anterior, incumple lo definido en el capítulo 3 de la Resolución 388 de 2019 "Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, se crea el Comité Institucional de Gestión y Desempeño y se dictan otras disposiciones", modificada por la Resolución 428 de 2021. Incumple lo señalado en la Ley 87 de 1993, articulo 2. Objetivos del Sistema de Control Interno, literal d. "*Garantizar la correcta evaluación y seguimiento de la gestión organizacional".* Literal e. *"Asegurar la oportunidad y confiabilidad de la información y de sus registros"*.

OBJECIONES PRESENTADAS POR EL PROCESO

Se precisa que el equipo técnico de Seguridad de la información durante la vigencia 2023, se ha reunido en dos ocasiones en las fechas del 25 de septiembre y 11 de octubre del presente año.

Evidencia:

Como evidencia de ello se encuentran las actas en proceso de aprobación para ser firmadas por los integrantes del equipo técnico, así como las grabaciones de las sesiones realizadas, que pueden ser consultadas en la ruta

Q:\12_SSI\Auditorias internas\Evidencias PM 2023\2.3

RESPUESTA A LA OBJECIÓN POR PARTE DE LA OFICINA DE CONTROL INTERNO

Analizados los soportes, se observan dos actas de reunión del Comité Técnico de Seguridad de la información con fecha 25 de septiembre de 2023 y 11 de octubre de 2023, las cuales están en formato Word sin firma de los asistentes, a espera de ser aprobadas y firmadas en próximo comité; igualmente, en la ruta se encuentran tres audios soporte de la primera reunión y un video de la segunda reunión, en las que se abordador temas del componente de Tecnologías de la Información y las Comunicaciones.

Sin embargo, estas reuniones se presentaron fuera del periodo auditado, lo que confirma la No conformidad 2.3. Por lo anterior, no se acepta la réplica y se debe formular el respectivo plan de mejoramiento.

Calificación del riesgo de la No conformidad

Probabilidad	Baja (40%)	**Impacto**	Moderado (60%)	**Calificación del Riesgo**	Moderado

3. OPORTUNIDADES DE MEJORA

3.1. Durante el periodo auditado se observó que la Corporación no contó con un responsable de seguridad de la información de manera permanente, para la vigencia 2023 se suscribió el contrato No. 230501 cuyo objeto es "*Prestar los servicios profesionales para apoyar el Proceso de Sistemas y Seguridad de la Información, en las actividades relacionadas con el Sistema de Seguridad de la Información del Concejo de Bogotá D.C.,*" vigencia 5 meses con adición de 27 días, el cual inicio el 05 de mayo de 2023 y finaliza el 01 de noviembre de 2023, es decir, durante el primer cuatrimestre, el Concejo de Bogotá no tuvo un responsable de seguridad de la información, lo cual ha generado atrasos en el cumplimiento de algunas responsabilidades del proceso en lo concerniente a las Políticas de Gobierno Digital y Seguridad Digital, así como la verificación y actualización de los procedimientos, guías, manuales y formatos del proceso SSI.

En este sentido, desde la Oficina de Control Interno se recomienda que, a través de los responsables se incorpore un funcionario Responsable de Seguridad de la Información de manera permanente, dada la importancia de este rol en la Corporación y teniendo en cuenta las funciones del cargo en el numeral 2 del Manual de Roles y Responsabilidades de Seguridad de la Información Código SSI-MA003.

3.2. Los indicadores de gestión para el segundo semestre de la vigencia 2022, solo el 49% de los casos solucionados respondieron la encuesta de satisfacción, se recomienda socializar y sensibilizar a los funcionarios para que las encuestas sean respondidas, las cuales son insumo importante para mejorar los servicios que brinda el proceso al interior de la corporación.

3.3. Con relación al plan de acción vigencia 2023 y luego de verificados los soportes, se recomienda adelantar las acciones necesarias para dar cumplimiento a las actividades; si bien es cierto, que algunas están en periodo de ejecución, presentan riesgo de no cumplimiento las actividades Nros.68, 80, 140, 141, 144, 147.

3.4. No hay evidencia de actualización del Normograma desde el último año, al cotejar el archivo de mayo de 2022 y el actual de agosto de 2023 publicado en la página web de la

corporación, no se evidencian actualizaciones del Normograma. Se recomienda constatar periódicamente la normatividad aplicable al proceso de Sistemas y Seguridad de la Información y realizar el reporte a la Dirección Jurídica de la Corporación.

3.5. Con relación a la información suministrada sobre el Manual de Políticas de Seguridad de la Información, se observó que en marco del contrato No. 230501 se realizará un informe que debe incluir, entre otros temas los siguientes: Seguimiento del proceso SSI a las políticas de dispositivos móviles, informe de cumplimiento de las Políticas de Seguridad y Privacidad de la Información. Se recomienda realizar seguimiento para dar cumplimiento a lo descrito en el manual.

3.6. Dado que el procedimiento SSI-PR002_Copias_Seguridad_BackUp se encuentra en proyecto de actualización y, al verificar el Manual de Políticas de Seguridad de la Información, se observa que el numeral 5.8 establece "*Los responsables de TI definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo*", lo cual debe estar alineado con el procedimiento SSI-PR002, se recomienda incluir esta actividad en el procedimiento y establecer un formato para registrar la información.

II. SSI-PR001 ADMINISTRACIÓN Y ACTUALIZACIÓN DE LA RED Y SERVIDORES

4. CONFORMIDADES

4.1. En respuesta y cumplimiento al procedimiento SSI-PR001, se da conformidad a lo descrito en el numeral 6.1 en lo referente a la verificación del funcionamiento de la plataforma tecnológica (Software, red, servidores, dispositivos de seguridad) a través de las consolas de administración de los activos de IT por el equipo de infraestructura tecnológica del proceso SSI; luego de verificados los soportes se observó que el proceso cuenta con las siguientes herramientas: FortiSIEM, Consola Oracle Cloud, StruxureWare Data Center Expert y Consola VMware, desde las cuales se realiza monitoreo al estado de los servidores y gestión de la capacidad, monitoreo a las Bases de Datos, a los cluster del sistema de hiperconvergencia y a los aires acondicionados y UPS.

4.2. De acuerdo con la información reportada, frente a la redundancia en los equipos activos de red y servidores, con el fin de garantizar la continuidad de los servicios de la infraestructura tecnológica, se evidenció que la Corporación cuenta con un sistema de hiperconvergencia, el cual presenta configuración de réplica entre las sedes del Concejo y el CAD; los servidores virtuales también cuentan con características de replicación de los nodos, los Switches de Core, el Firewall y Web Application Firewall WAF, también cuentan con redundancia, lo cual aumenta la disponibilidad en la infraestructura critica en la Corporación.

4.3. De acuerdo con la información reportada, se da conformidad a lo solicitado frente al establecimiento y administración de privilegios para el acceso a los sistemas de información de la Corporación, se pudo constatar que estos se asignan al crear las cuentas de usuario o por solicitudes de modificación del jefe inmediato. Para otro tipo de sistemas como CORDIS, LIBREJO, FILESERVER o acceso a la red corporativa por VPN, se realiza a través de solicitud del jefe de la dependencia.

5. NO CONFORMIDADES

5.1. No se evidenciaron.

6. OPORTUNIDADES DE MEJORA

6.1. El formato SSI-PR001-FO1 no cuenta con información que permita saber que funcionario realizó actividades de verificación a la infraestructura, tampoco se puede evidenciar a que activo de información específicamente se le realizó verificación, en el formato se describe de manera general (Servidores, Storage, Comunicaciones). Se recomienda actualizar el formato e incluir información relevante que permita determinar de manera puntual el activo de información, verificación o tarea realizada y funcionario del proceso SSI que lo realiza.

6.2. Se recomienda realizar las actividades necesarias para la actualización del procedimiento, del cual se evidenció un documento en proyecto, pero no cuenta con la respectiva revisión metodológica de la Oficina Asesora de Planeación para su posterior presentación en el Comité Institucional de Gestión y Desempeño.

III. SSI-PR003 ATENCIÓN DE SOPORTE TECNOLÓGICO

7. CONFORMIDADES

7.1. En respuesta y cumplimiento a lo solicitado, frente a los Acuerdo de Niveles de Servicio suscritos en el contrato No. 230427 de mesa de servicios y, luego de revisados 4 informes de gestión correspondientes a los periodos de 13 de abril a 12 de mayo, 13 de mayo a 12 de junio, 13 de junio a 12 de julio y 13 de julio a 12 de agosto de 2023, se evidencia cumplimiento a los acuerdos de niveles de servicio estipulados en el acuerdo marco, que no dieron lugar a aplicar sanciones económicas sobre la facturación.

7.2. Durante la vigencia del contrato No. 230427 de mesa de servicios con SELCOMP INGENIERIA SAS, no se ha presentado indisponibilidad del Software de mesa de servicios ARANDA, que hubiera dado lugar a recibir solicitudes por otro medio distinto al software dispuesto. Al revisar los informes de gestión de abril a agosto de 2023 se observan los medios de recepción de los casos y las cantidades; por lo anterior, se da conformidad a lo descrito en el numeral “6.1.1 Recibir Solicitud” del procedimiento SSI-PR003.

7.3. Se da conformidad a lo solicitado en la pregunta 36 del cuestionario de auditoria, relacionado con el plan de mantenimiento preventivo con ocasión del contrato No. 230427 con SELCOMP INGENIERIA SAS, mantenimiento que inicio el día 18 de septiembre de 2023, actualmente se encuentra en ejecución.

8. NO CONFORMIDADES

8.1. No se evidenciaron.

9. OPORTUNIDADES DE MEJORA

9.1. Se recomienda realizar seguimiento a los casos en estado suspendido, avisar o notificar a los usuarios el tiempo en que posiblemente se dará solución y las razones por las cuales no se da solución en los tiempos establecidos, en el mismo sentidos, realizar seguimiento a los casos escalados a 3er nivel.

9.2. Se recomienda realizar las actividades necesarias para la actualización del procedimiento, en el que se incluya entre otras los canales autorizados para recepción de casos, del cual se evidenció un documento en proyecto, pero no cuenta con la respectiva revisión metodológica de la Oficina Asesora de Planeación para su posterior presentación en el Comité Institucional de Gestión y Desempeño.

9.3. Se recomienda fortalecer la herramienta de base conocimiento, con el fin de documentar y compartir la información de soporte técnico que puede ser útil tanto para el usuario final como para el personal de soporte.

9.4. Con el propósito de mejorar la satisfacción del usuario, se recomienda sensibilizar al usuario final luego de atender el soporte para que diligencien la encuesta de satisfacción, dado que al revisar los indicadores de gestión, se observó que en el segundo semestre de 2022, solo el 49% de los casos solucionados respondieron la encuesta.

IV. SSI-PR005 PLAN DE NECESIDADES DE CONTRATACIÓN Y SEGUIMIENTO A LOS CONTRATOS DE TECNOLOGÍA

10. CONFORMIDADES

10.1. Se realiza el análisis de conformidad a la pregunta 37 según cuestionario de auditoria, frente al seguimiento del formato Código: SSI-PR005-FO3, se pudo observar que se aplicó el seguimiento a 40 contratos para el 2022, de los cuales el concepto de EJECUTADOS fueron 29, en EJECUCIÓN 11. Para el periodo 2023 se remitieron 13, de los cuales los mismos se encuentran en EJECUCIÓN.

Contratos 2022	Contratista	Valor del Contrato	Estado Contractual
N° 220323	ALEZ YOBANI BOCIGA PEÑA	$ 30.096.000,00	EJECUTADO
N° 220338	ROBINSON MELO MORENO	$ 13.956.000,00	EJECUTADO
N° 220354	GUILLERMO ANTONIO SILVA QUEVEDO	$ 11.166.000,00	EJECUTADO
N° 220382	TANDEM S.A.S	$ 4.091.910,00	EJECUTADO
N° 220391	SELCOMP INGENIERIA S A S (SISTEMAS Y ELECTRONICA DE COMPUTADORES)	$ 169.504.743,00	EJECUTADO
N° 220397	HACHI S A S	$ 49.244.823,00	EJECUTADO
N° 220400	COMPAÑIA COMERCIAL CURACAO DE COLOMBIA S .A.	$ 8.535.180,00	EJECUTADO
N° 220403	EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. E.S.P. - ETB S.A. ESP	$ 46.845.336,00	EJECUTADO
N° 220405	GRAN IMAGEN S.A.S.	$ 98.252.136,00	EJECUTADO
N° 220426	RGS REDES Y COMUNICACIONES SAS	$ 40.170.000,00	EJECUTADO
N° 220431	RUTH CAROLINA ALVAREZ MOJICA	$ 27.912.000,00	EJECUTADO
N° 220437	INFORMATICA DOCUMENTAL	$ 12.600.000,00	EJECUTADO
N° 220454	ALEZ YOBANI BOCIGA PEÑA	$ 25.080.000,00	EJECUTADO
N° 220491	KHAANKO NORBERTO RUIZ RODRIGUEZ	$ 20.160.000,00	EJECUTADO
N° 220574	UNION TEMPORAL WEX-LOCK-DRP 2022	$ 249.907.970,00	EJECUTADO
N° 220581	FACTOR VISUAL	$ 50.000.000,00	EJECUTADO
N° 220588	ROBINSON MELO MORENO	$ 9.304.000,00	EJECUTADO
N° 220673	GUILLERMO ANTONIO SILVA QUEVEDO	$ 8.374.500,00	EJECUTADO
N° 220674	UNION TEMPORAL NIMBIT	$ 391.126.207,00	EJECUTADO
N° 220754	WEXLER SAS	$ 249.103.890,00	EJECUTADO
N° 220773	UNIPLES	$ 91.075.236,00	EJECUTADO
N° 220774	VASQUEZ CARO Y CIA SAS	$ 13.878.105,00	EJECUTADO
N° 220775	UNIPLES	$ 334.796.806,00	EJECUTADO
N° 220785	SISTETRONICS SAS	$ 43.748.684,00	EJECUTADO
N° 220837	TALENTO SOLIDO S.A.S	$ 182.473.612,00	EJECUTADO
N° 220860	FACTOR VISUAL	$ 3.950.000,00	EJECUTADO
N° 220873	TEAM MANAGEMENT INFRASTRUCTURE S.A.S	$ 334.549.411,00	EJECUTADO
N° 220881	GESTION DE SEGURIDAD ELECTRONICA S.A	$ 21.420.000,00	EJECUTADO
N° 220885	APROVISIONAR SOLUCIONES SAS	$ 20.433.578,00	EJECUTADO
TOTAL		$ 2.561.756.127,00	

Contratos 2022	Contratista	Valor del Contrato	Estado Contractual
N° 220445	ETB (EDIFICO NUEVO)	$ 3.250.551.965,00	EN EJECUCION
N° 220529	GREEN FON GROUP S A S	$ 31.736.762,00	EN EJECUCION
N° 220577	BRANCH OF MICROSOFT COLOMBIA INC	$ 265.968.099,00	EN EJECUCION
N° 220568	INGEAL S A	$ 211.877.000,00	EN EJECUCION
N° 220776	SOLUCIONES ORION SUCURSAL COLOMBIA	$ 263.512.432,00	EN EJECUCION
N° 220800	SOLUCIONES ICG	$ 79.433.432,00	EN EJECUCION
N° 220816	BMIND	$ 188.408.677,00	EN EJECUCION
N° 220845	SANOLIVAR S A S	$ 282.138.000,00	EN EJECUCION
N° 220887	MATIZZO SAS MANTENIMIENTO COMUNEROS	$ 200.000.000,00	EN EJECUCION
N° 220893	MATIZZO SAS NUEVO EDIFICIO	$ 9.890.000.000,00	EN EJECUCION
N° 220900	DAYSCRIPT S A S EN REORGANIZACION	$ 278.000.000,00	EN EJECUCION
TOTAL		$14.941.626.367,00	

Contrato 2023	Contratista	Valor del Contrato	Estado Contractual
230327	HACHI SAS	$ 63.222.327,00	EN EJECUCION
230367 Numero de orden de Compra 106668	ETB (Conectividad)	$ 55.099.451,00	EN EJECUCION
230427 Número Orden de Compra 107180	SELCOMP INGENERIA SAS	$ 308.756.442,00	EN EJECUCION
230501	KHAANKO NORBERTO RUIZ RODRIGUEZ	$ 20.160.000,00	EN EJECUCION
230504	MARCO AURELIO CUMBE ANDRADE	$ 16.285.000,00	EN EJECUCION
230508	WEXLER S.A.S	$ 533.988.000,00	EN EJECUCION
230570	ALEZ YOBANI BOCIGA PEÑA	$ 25.080.000,00	EN EJECUCION
230593	FACTOR VISUAL EAT	$ 75.000.000,00	EN EJECUCION
230610	GRAN IMAGEN S.A.S	$ 201.502.956,00	EN EJECUCION
230697	UNIPLES S.A	$ 20.579.400,00	EN EJECUCION
230733	DIGICOM SYSTEM CORPORATION S A	$ 5.201.194,00	EN EJECUCION
230749	BIT512 SOLUCIONES TI S A S	$ 130.897.620,00	EN EJECUCION
230846	INFORMATICA DOCUMENTAL SAS	$ 14.570.388,00	EN EJECUCION
TOTAL		$ 1.470.342.778,00	

11. NO CONFORMIDADES

11.1. No se evidenciaron.

12. OPORTUNIDADES DE MEJORA

12.1. Se recomienda realizar las actividades necesarias para la actualización del procedimiento, del cual se evidenció un documento en proyecto, pero no cuenta con la respectiva revisión metodológica de la Oficina Asesora de Planeación para su posterior presentación en el Comité Institucional de Gestión y Desempeño.

V. SSI-PR009 ACCESO FÍSICO A LAS INSTALACIONES E INGRESO DE EQUIPOS PORTÁTILES

13. CONFORMIDADES

13.1. De acuerdo a reunión de apertura de auditoria al proceso SSI el día 24 de agosto de 2023, en la que el proceso manifestó que para el procedimiento SSI-PR009 solicitaron traslado al proceso Gestión de Recursos Físicos, argumentando que el procedimiento se encuentra más asociado a actividades de gestión de la seguridad física, ingreso de personas y elementos a las instalaciones de la Corporación, lo cual se aborda de forma más directa en los puntos de control de acceso a través del servicio de vigilancia.

De lo anterior, y luego de verificar los soportes enviados, se evidencia correo electrónico de fecha 13 de abril de 2023 a la Oficina Asesora de Planeación solicitando acompañamiento para reformular y dar traslado del procedimiento, en el correo electrónico anexa: Memorando de la Dirección Administrativa a la OAP, formato GMC-FO-001_Solicitud_actualizacion_documental.TrasladoPR009-f.pdf y formato GMC-FO-

001_Solicitud_actualizacion_documental.TrasladoPR009.xlsx, por lo tanto se da conformidad a lo solicitado en el cuestionario de auditoria.

14. NO CONFORMIDADES

14.1. No se evidenciaron.

15. OPORTUNIDADES DE MEJORA

15.1. Se evidencia gestión del proceso para dar traslado del procedimiento al proceso Gestión de Recursos Físicos, sin embargo, no se ha hecho efectivo el traslado y tampoco se evidencia seguimiento de la solicitud, por lo anterior, se recomienda realizar seguimiento, entendiendo que hasta tanto no se oficialice el traslado, es responsabilidad del proceso SSI dar cumplimiento a lo descrito en el mismo, así como las modificaciones o actualizaciones.

VI. SSI-PR010 ACCESO LÓGICO

16. CONFORMIDADES

16.1. Se da conformidad a lo solicitado, frente a qué mecanismos de seguridad se utilizan en la entidad para evitar la conexión de equipos no institucionales a la red cableada; se pudo confirmar que los Switches de acceso presentan configuración de seguridad por puertos o port-security, con la cual se bloquea la conexión de dispositivos no autorizados, en el caso de que servidores o visitantes conecten equipos no institucionales a los puertos de red en la Entidad.

16.2. Se da conformidad a la pregunta No. 45 del cuestionario relacionada con el acompañamiento y control que el proceso SSI aplica a los proveedores de servicio que brindan soporte en sitio y remoto a la infraestructura de tecnología en la Entidad. Luego de verificados los soportes, se evidenció que con la legalización de los contratos se suscriben los respectivos acuerdos de confidencialidad.

17. NO CONFORMIDADES

17.1. No se evidenciaron.

18. OPORTUNIDADES DE MEJORA

18.1. De acuerdo a verificación realizada de manera aleatoria a los equipos de cómputo en la diferentes dependencias de la Corporación, se observa que los equipos cuentan con un usuario administrador local, sin embargo, estos no se encuentran estandarizados, se recomienda, en coordinación con el contrato de mesa de servicios realizar esta actividad con el propósito de corroborar lo descrito en la respuesta a la pregunta No. 40 del cuestionario de auditoria "*las contraseñas se estandarizan durante los mantenimientos preventivos y se entregan al acompañamiento técnico del contrato*", a razón de que en este momento se está llevando a cabo el mantenimiento preventivo de equipos en la Entidad.

18.2. El procedimiento no contempla el acceso a las redes inalámbricas y conexiones a través de una Red Privada Virtual VPN, se recomienda incluir lineamientos para el uso y control de estas tecnologías en el procedimiento.

18.3. Se recomienda realizar las actividades necesarias para la actualización del procedimiento, del cual se evidenció un documento en proyecto, pero no cuenta con la respectiva revisión metodológica de la Oficina Asesora de Planeación para su posterior presentación en el Comité Institucional de Gestión y Desempeño.

VII. SSI-PR011 GESTIÓN DE ACTIVOS

19. CONFORMIDADES

19.1. En respuesta y cumplimiento a lo solicitado, se da conformidad a la pregunta No. 46 del cuestionario, en la que se solicitó información relacionada con el Oficial de Seguridad, se observó acta de iniciación del contrato No. 220491 cuyo objeto fue Prestar los servicios profesionales para apoyar el Proceso de Sistemas y Seguridad de la Información, en las actividades relacionadas con el Sistema de Seguridad de la Información del Concejo de Bogotá D.C., vigencia del contrato del 23/08/2022 al 31/12/2022, así mismo se evidencio en SECOP el contrato No. 230501 con el mismo objeto del anterior, vigencia de 5 meses, fecha de inicio 05/05/2023, con un adición de 27 días hasta el 01/11/2023.

20. NO CONFORMIDADES

20.1. No se evidenciaron.

21. OPORTUNIDADES DE MEJORA

21.1. Actualmente el proceso SSI tiene No conformidades derivadas de auditorías anteriores, relacionadas con la Gestión de Activos de Información y, teniendo en cuenta que al revisar los soportes enviados sobre el inventario de los Activos de Información, estos se observan incompletos, se recomienda realizar las actividades necesarias en coordinación con el Oficial de Seguridad para darle cumplimiento a lo descrito en el procedimiento SSI-PR011, numerales: 6.1 IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN, 6.2 VALORAR LOS ACTIVOS DE INFORMACIÓN Y 6.3 ACTUALIZAR EL INVENTARIO DE ACTIVOS.

21.2. Con relación al inventario de activos de tecnología de la Corporación, y en el mismo sentido del informe de derechos de autor vigencia 2022, se recomienda realizar una revisión y verificación en las instalaciones de la Entidad, con el fin llevar un control de elementos tecnológicos (Computadores de escritorio, portátiles, servidores, licencias de software, entre otros) al interior del Concejo de Bogotá, y de esta manera, garantizar la confiabilidad de la información, en cuanto a la cantidad de equipos y licencias de software reportadas por la Secretaria de Hacienda Distrital, para efectos de determinar las diferencias y actualizar la información, de tal forma, que las dos Entidades puedan coadyuvar en identificar plenamente la totalidad de activos, y dar mayor confiabilidad a la información reportada.

VIII. VERIFICACIÓN DE PLANES DE MEJORAMIENTO DERIVADOS DE AUDITORIAS ANTERIORES (Seguimiento correspondiente al segundo trimestre de 2023, presentado el 01 de septiembre de 2023).

NO CONFORMIDAD 10.2.2 DE 2019. Se evidenció que el inventario de activos de información no se encuentra actualizado debido a que el documento publicado en la Intranet de la Corporación corresponde al 24 de noviembre de 2017 y está incompleto, porque no están diligenciados los campos idioma, medio de conservación y/o soporte, formato, información, custodio de la información, clasificación y valoración del activo, valor del activo y forma de etiquetar para los procesos de Comunicación e Información, Evaluación Independiente, Mesa Directiva, Mejora Continua, Gestión Documental, Gestión Financiera, Gestión Jurídica y Talento Humano.

Además, se estableció que al diligenciar el formato SSI-PR008-F01 para presentar el inventario de hardware, software y servicios, el Proceso de Sistemas y Seguridad de la Información le eliminó los campos de "Clasificación y valoración de activos" y "Forma de etiquetado" y agregó el campo "Ubicación del activo". Situación que no debió suceder dado que éste es un formato oficial del SIG y no se puede alterar.

ACCIÓN PROPUESTA. Actualizar la información del inventario de activos de información.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2019\10.2.2\Actividades 2023, el archivo "*Inventario Activos de Información y Riesgos CB_V1.xlsx*", de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Dentro del inventario de activos de información que se relaciona en este hallazgo, se ha coordinado con los líderes de los procesos que aún hacen falta tramitar (Gestión Normativa, Control Político, Gestión Documental y Atención al Ciudadano) para que se entregue la información actualizada y de esta forma cumplir con los compromisos adquiridos para dar cierre a esta acción correctiva.*
Por lo anterior, a la fecha se informa de la actualización del inventario de activos de información de los procesos "Gestión Documental", "Gestión Normativa" y "Control Político" labor que se puede ratificar en el documento que compartimos en la red corporativa. Así mismo, se evidencia el agendamiento realizado en el primer semestre del año en curso a los líderes de los procesos "Gestión Normativa y Control Político" y que tuvo como finalidad realizar el seguimiento a este punto específico.
Finalmente, se manifiesta que la SSI tiene toda la disposición a seguir trabajando para finalizar la consolidación de los activos de información del proceso de "Atención al Ciudadano".

Analizados los soportes en la ruta indicada, se observa en el archivo Excel "Inventario Activos de Información y Riesgos CB_V1.xlsx" que los activos de información de Gestión Documental ya se encuentran incluidos en el documento, sin embargo, los activos de información de Gestión Normativa, Control Político y Atención al Ciudadano no están completamente diligenciados.

Por otro lado, no se ha realizado retroalimentación luego del diligenciamiento de la matriz de activos de información.

CONCLUSION. De acuerdo a la verificación de la información dispuesta en la red interna indicada por el Proceso de Sistemas y Seguridad de la Información, se otorga un avance del 60% en el cumplimiento de la acción concertada. Abierta 3 años y 11 meses.

NO CONFORMIDAD 10.2.5 DE 2019. Se verificó que en la Corporación no se está aplicando el Procedimiento de Clasificación, Etiquetado y Manejo de la Información SSI-PR008 versión 3 del 11 de diciembre de 2018, el cual está definido por el Proceso de Sistemas de Seguridad de la Información, para un adecuado etiquetado y manejo de la información física y digital, de acuerdo

con su clasificación. Lo anteriormente enunciado, incumple el control A.8.2.2 Etiquetado de la Información "Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la Información, de acuerdo con el esquema de clasificación de información adoptado por la organización" establecido en la Norma ISO 27001:2013 Sistema de Gestión de Seguridad de la Información.
ACCIÓN PROPUESTA. Actualizar el procedimiento de Clasificación, etiquetado y manejo de la información junto con el proceso de Gestión Documental.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2019\10.2.5\Actividades 2023, el archivo "*SSI-PR004 Administración Activos de TI V.05.docx*" de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Teniendo en cuenta la "Guía para la Gestión y Clasificación de Activos de Información" número 5 publicada por MINTIC, se coordina con el responsable de seguridad de la Información, actualizar el documento "unificando" este procedimiento de gestión, clasificación, etiquetado y manejo de los activos de información en uno solo. Por tal motivo, se desarrollan los últimos ajustes de validación al documento "SSI-PR008_Clasificacion_Etiquetado_y_Manejo_Informacion V.04 En Actualización" el cual se encuentra en validación por parte del proceso de Sistemas con el fin de solicitar la aprobación metodológica a la O.A.P. así mismo, compartir con la O.C.I. todos los avances que se tengan al respecto, con el propósito de lograr el cierre de esta No Conformidad.* *Por último, se comparte la "Matriz de Inventario y Clasificación de Activos de Información" propuesta por MINTIC la cual se encuentra en proceso de ajuste para ser adoptada por el Concejo de Bogotá y así estar alineados a todas las estrategias tecnológicas que imparte dicho Ministerio y de esta forma realizar una adecuada identificación de los activos de información*." Se verifico el procedimiento en proyecto y, al igual que en el seguimiento realizado a la acción en el primer trimestre de 2023 de acuerdo a memorando 2023IE7913, se observa que el documento tiene fecha de control de cambios enero de 2023, pero no hay evidencia de envío a la Oficina Asesora de Planeación para su revisión metodológica.
CONCLUSION. En conclusión y, luego de verificar los soportes, la acción continúa con un avance del 50% de cumplimiento. Abierta 3 años y 10 meses.
NO CONFORMIDAD 10.2.14 DE 2019. Se observó que el Sistema de Gestión de la Seguridad de la Información ha sido evaluado por la auditoría externa a cargo de Password, examinado por la Certificadora SGS, analizado por el Comité SIG No. 13 efectuado el 13 de diciembre de 2017 (Revisión por la Dirección) y diagnosticado sobre el cumplimiento de la NTC ISO 27001:2013 por la Oficina Asesora de Planeación de la Corporación, de cuyas verificaciones se determinaron No Conformidades y sugerencias para que el sistema se ajuste a los requerido por la Norma ISO 27001:2013 y propender por la mejora continua del mismo. Sin embargo, no se evidencia dicha mejora porque las acciones implementadas no atacan las causas que los originan, están desarticuladas con el Sistema de Gestión de Seguridad de la Información y con el Sistema Integrado de Gestión de la Corporación, lo que genera su ineficacia.
ACCIÓN PROPUESTA. Realizar el seguimiento a los planes de mejoramiento del proceso y del SGSI.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2019\10.2.5\Actividades 2023, de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Para cada una de las actividades propuestas o descritas en el Plan de Mejoramiento Institucional, SSI realiza los seguimientos correspondientes a todas las "No conformidades" descritas anteriormente. Como*

evidencia de estos trabajos, se puede observar los avances documentados y señalados en cada una de las rutas reseñadas en la red corporativa.

El propósito final de SSI es cumplir con la eficacia de todas las tareas propuestas y de esta forma solicitar el cierre a cada una de las "No conformidades" establecidas en las Auditorías Internas ejecutadas por la OC.I"

Consultados los soportes, se evidencia el seguimiento que el proceso SSI ha realizado al plan de mejoramiento de 2019, sin embargo, las No conformidades 10.2.2 y 10.2.5 de 2019 continúan abiertas y con un porcentaje de avance de 60% y 50% respectivamente. Con el cierre de estas No conformidades, se daría finalización a la 10.2.14 de 2019.

CONCLUSION. En conclusión y, luego de verificados los soportes de seguimiento a los planes de mejoramiento de las No conformidades vigencia 2019, se otorga un avance del 60% de cumplimiento a la acción. Abierta 3 años y 5 meses.

NO CONFORMIDAD 2.5 DE 2020. Se observó que el software de mesa de ayuda no está disponible para cumplir con la actividad de realizar el "Registro de las Lecciones Aprendidas" derivadas de la ocurrencia de los incidentes de seguridad, con el propósito de conocer:
- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Cuál sería la gestión del personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Actualización de la matriz de riesgos.
- Acciones correctivas para prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro

En consecuencia, se puede perder información valiosa para la adecuada gestión de los incidentes de seguridad.

ACCIÓN PROPUESTA. Se realizará una actualización del procedimiento y se determinará cuando se considera que un incidente es grave.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Consultada la documentación en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2020\2.5\Evidencias 2023\ SSI-PR007_Gestion_Incidentes_Seguridad_Informacion V.04.docx, de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Con el propósito de contar con un procedimiento estructurado y bien planificado el cual permita manejar adecuadamente los incidentes de seguridad de la información, SSI trabaja con el profesional de seguridad para que este documento "SSI-PR007 procedimiento gestión de incidentes de seguridad de la información" se encuentre homologado con los últimos lineamientos establecidos y priorizados por esta área. Al momento de confirmar que este archivo cuenta con todos los vistos buenos, se solicitará la aprobación metodológica a la O.A.P, Así mismo, se enviarán todas las evidencias a la O.C.I.*
Finalmente, se comparte a la OCI el último documento que tenemos para que se valide los avances de cumplimiento de las acciones indicadas en el plan de mejoramiento y que ayudarán a el cierre de esta No Conformidad."

Se verifico el procedimiento en proyecto, el cual tiene fecha de control de cambios marzo de 2023, pero no ha sido enviado a la Oficina Asesora de Planeación para su revisión.

CONCLUSION. En conclusión y, luego de verificar los soportes, la acción continúa con un avance del 50% de cumplimiento. Abierta 2 años y 5 meses.

NO CONFORMIDAD 2.8 DE 2020. Se estableció que el Proceso de Sistemas y Seguridad de la Información no actualizó sus 13 procedimientos en el 2019, como lo programó la Oficina Asesora de Planeación, entre otros, aspectos para diseñar los controles de acuerdo con los lineamientos1 de la Guía para la Administración de Riesgos y Definición de Controles en Entidades Públicas versión 4 emitida por el DAFP y así facilitar la aplicación de la metodología de administración de riesgos.
En consecuencia, los controles utilizados en el proceso de gestión de riesgos no son robustos para mitigar los riesgos y evitar su materialización.

ACCIÓN PROPUESTA. Se realizará la actualización y ajuste de ser necesario de los procedimientos del Proceso para su presentación y aprobación por parte del CIGD.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2020\2.8\Actividades 2023, de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Para el cumplimiento de estas acciones que se propusieron en el plan de Mejoramiento, SSI coordinó internamente para que se tengan actualizados los procedimientos "SSI-PR002 y el SSI-PR009" (Realización Copias de Seguridad Backup y el Acceso Físico a las Instalaciones e Ingreso de Equipos Portátiles, respectivamente) y de esta forma ejecutar todas las tareas detalladas en el anterior plan. Así mismo, SSI realizó la solicitud de traslado al procedimiento SSI-PR009 y la solicitud de actualización al procedimiento SSI-PR002 y la petición de modernización documental para este último archivo.*

Por lo anterior, SSI da como evidencias documentales los siguientes archivos que sustentan las labores anteriormente indicadas:

- *Solicitud actualización documental (GMC-F0-001)*
- *Correos donde se evidencian las solicitudes internas realizadas.*
- *Documento actualizado SSI-PR002_Copias Seguridad BackUp V.10 (2)*
- *Documento actualizado SSI-P00R009 Acceso Físico a Instalaciones Ingreso Equipo Portátiles V. 04*

Finalmente, SSI reportará a la OCI todos los progresos que se tenga para poder subsanar este hallazgo identificado en la Autoría Interna."

Consultados los soportes, se observa dos formatos GMC-FO-001 de fechas 14/03/2023 y 13/04/2023 con solicitud de modificación del documento SSI-PR002 Realización Copias de seguridad Backup, sin firma del líder del proceso ni evidencia de envío a la Oficina Asesora de Planeación. Así mismo, se observan 10 procedimientos con control de cambios así:

SSI-PR001 enero 2023, SSI-PR002 20 de febrero de 2023, SSI-PR003 febrero 2023, SSI-PR004 enero 2023, SSI-PR005 enero 2023, SSI-PR006 enero 2023, SSI-PR007 marzo 2023, SSI-PR009 enero 2022, SSI-PR010 18 de marzo de 2022, SSI-PR012 enero 2023. De estos procedimientos no hay soporte de envío a la OAP para su revisión metodológica.

CONCLUSION. En conclusión y, luego de verificar los soportes, se observa que a pesar de tener los procedimientos en proyecto de modificación, estos siguen desactualizados sin evidencia de envío a la OAP, por lo tanto, se otorga un avance del 60% de cumplimiento de la acción. Abierta 2 años y 2 meses.

NO CONFORMIDAD 8.3 DE 2020. Se observó incumplimiento en el botón de transparencia del numeral 10.2. Registro de Activos de Información apartado b, ya que a la fecha no se encuentra publicado el Registro de Activos de Información en la portal www.datos.gov.co, generando así incumplimiento del artículo 38 del Decreto 103 de 2015 referido a "*El Registro de Activos de*

Información debe elaborarse en formato de hoja de cálculo y publicarse en el sitio web oficial del sujeto obligado, así como en el Portal de Datos Abiertos del Estado colombiano o en la herramienta que lo modifique o lo sustituya."
ACCIÓN PROPUESTA. El día 19 de septiembre de 2020 se realizó la actualización de la información en el portal de datos abiertos, se propone como acción de mejora actualizar la matriz de activos de la información y realizar su publicación en el portal corporativo y en el de datos abiertos.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2020\8.3\Actividades 2023, de acuerdo a memorando 2023IE11371 remitido a la Oficina de Control Interno; al igual que en la No conformidad 10.2.2 de 2019, se observa en el archivo Excel "*Inventario Activos de Información y Riesgos CB_V1.xlsx*" que los activos de información de Gestión Documental ya se encuentran incluidos en el documento, sin embargo, los activos de información de Gestión Normativa, Control Político y Atención al Ciudadano no están completamente diligenciados.
CONCLUSION. En este sentido, luego de la verificación de la información dispuesta en la red interna indicada por el Proceso de Sistemas y Seguridad de la Información y, teniendo en cuenta que, el documento Matriz de Activos de Información debe estar actualizado para su publicación, lo cual está pendiente de acuerdo a la No conformidad 10.2.2 de 2019, se otorga un avance del 60% en el cumplimiento de la acción concertada. Abierta 2 años y 2 meses.
NO CONFORMIDAD 2.1 DE 2022. Se evidenció, que el procedimiento "Realización de copias de seguridad backup", numeral 6.8. "El Auxiliar Administrativo marca las cintas de forma organizada con los parámetros de almacenamiento entregados por el Profesional Universitario como lo es: Fecha del backup, nombre del servidor y nombre de trabajo de Backup y se almacenan en cintoteca", no es realizada por el auxiliar administrativo según respuesta entregada por la Dirección, en donde indican que: "La marcación de cintas no se está realizando por parte del el Auxiliar Administrativo; toda vez, el proceso de SSI no cuenta con este recurso asignado. Esta actividad la realiza el profesional universitario". Se determinó que el numeral 6.9, "El Auxiliar Administrativo registra en la bitácora de copias de seguridad el Tipo de Sesión, Esp, Estado, Modo Backup, Total Incremental, Tiempo de Inicio, En cola, Duración, GB Escritos, N° Cintas, No Errores, No Advertencias, N° Archivos, Avance y ID de la Sesión; según formato (SSI-PR002-FO1) el cual se lleva en formato Excel y de forma local en equipo". Tampoco es desarrollada por un auxiliar administrativo dado que, en su respuesta indicaron: "Por cuanto no se cuenta con este recurso, la actividad del registro en la bitácora, la está haciendo el Profesional Universitario". Tanto el numeral 6.8 y 6.9, son resultado de la falta de la Revisión y Actualización del Procedimiento, porque lleva a no ejecutarse de acuerdo a la descripción del mismo.
ACCIÓN PROPUESTA. Se realizará la actualización y se presentará para su aprobación del CIGD el procedimiento Realización de copias de seguridad backup. Se solicitará a Talento Humano completar el equipo de trabajo en el proceso de Sistemas y Seguridad de la Información. Se asignará la tarea de marcación de cintas a un Auxiliar Administrativo asignado al proceso.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2022\2.1\Evidencias 2023, de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*SSI trabaja internamente para dar respuesta a las acciones indicadas en el Plan de Mejoramiento y de esta forma subsanar el hallazgo identificado, por consiguiente, se indica que a la fecha de este informe se ha ejecutado los siguientes trabajos que demuestran los avances que se tiene al respecto:*

1. Contamos con la versión Nro. 10 del procedimiento "Realización de copias de seguridad backup"
2. Formato de restauración copias de seguridad actualizado
3. Solicitud actualización documental - SSI-PR002 -Realización Copias de seguridad Backup
4. Solicitud actualización documental - SSI-PR002-FO1
5. Se comparte copia del memorando dirigido a la Oficina Asesora de Planeación con el propósito de requerir la revisión y aprobación metodológica del ProcedimientoSSI-PR002 (Realización copias de seguridad Backup)
6. Se comparte el documento actualizado "Bitácora copia de Seguridad Backups, formato SSI-PR002-FO1
7 .Se comparte una Imagen de la lista de sesiones realizadas.

Finalmente, y como lo indicamos anteriormente, la SSI trabaja internamente en conjunto para lograr el objetivo final que es cumplir con todo lo establecido y de esta forma solicitar el cierre de este Hallazgo. Así mismo, al momento de obtener otras evidencias de avances que ayude a la meta deseada, se informará inmediatamente a la O.C.I."

Verificados los soportes, se evidencia proyecto de la versión del Nro. 10 del procedimiento "*Realización de copias de seguridad backup*", última fecha de control de cambios 20 de febrero de 2023 y los documentos relacionados, sin embargo, los formatos GMC-FO-001 y el memorando con asunto: "*Solicitud revisión metodológica Procedimiento para aprobación*", en el cual adjuntan los documentos mencionados, no tienen la firma del líder del proceso y el memorando tampoco tiene radicado en CORDIS, es decir, no se puede comprobar el envío a la OAP.

CONCLUSION. Por lo anterior, y teniendo en cuenta que ya hay un procedimiento en proyecto con los formatos, se otorga un avance del 60% de cumplimiento a la acción concertada. Abierta 5 meses.

NO CONFORMIDAD 2.2 DE 2022. Dentro del procedimiento "Atención de soporte tecnológico", se pudo verificar que la entidad no cuenta con un plan de mantenimiento como lo indica el numeral 6.6. Informes y estadísticas "El contrato de mesa de ayuda debe contar con un plan de mantenimiento (Planilla Mantenimiento Preventivo Equipo – SSI-PR003-FO2), el cual debe ser revisado y aprobado por el encargado del proceso de Sistemas y Seguridad de la Información".
Analizada la respuesta por la Dirección, indicando que "El contrato de mesa de servicios incluye los mantenimientos preventivos, y tanto el procedimiento como el formato se encuentran en revisión para ser actualizados, los mantenimientos se registran en un formato acordado con el contratista de mesa de servicios que contiene mucha más información".

ACCIÓN PROPUESTA. Se realizará la actualización y se presentará para su aprobación del CIGD el procedimiento de Atención de soporte tecnológico.
Se realizará la actualización y/o cambio del formato SSI-PR003-FO2 Planilla mantenimiento preventivo de equipos.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Auditorias internas\Evidencias PM 2022\2.2\Evidencias 2023, de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Teniendo en cuenta la descripción indica en el Plan de Mejoramiento, la SSI ha actualizado el Procedimiento "Atención de Soporte Tecnológico" (SSI-PR003) a la versión 9, cuyo objetivo es "Realizar la atención de incidentes y requerimientos, teniendo en cuenta los acuerdos de niveles de servicio establecidos, para garantizar el correcto funcionamiento de la plataforma tecnológica dispuesta para los servidores públicos, para el cumplimiento de sus funciones", por lo que la unidad proyecta todas las labores necesarias para solicitar a la O.A.P. la revisión y aprobación metodológica. Por lo anterior, SSI comparte los siguientes documentos los cuales se tienen actualizados a la fecha:*

• *Procedimiento Atención de Soporte Tecnológico (SSI-PR003)* • *Plan de Mantenimiento Preventivo y Correctivo Infraestructura Tecnológica* • *SSI-PR003-F02V2, Formato para Planilla Mantenimiento EQs."* Verificada la información, se observa la actualización del procedimiento en proyecto con fecha de control de cambios julio de 2023, formato SSI-PR003-FO2 "PLANILLA MANTENIMIENTO PREVENTIVO EQUIPO" y documento en Word "PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO A INFRAESTRUCTURA TECNOLÓGICA". Tampoco se evidencia soporte de envío a la OAP.
CONCLUSION. Por lo anterior, y luego de verificar los soportes, se otorga un avance del 50% de cumplimiento. Abierta 5 meses.
NO CONFORMIDAD 3.1.1.1 AUDITORIA DE REGULARIDAD CONTRALORÍA 2021. Hallazgo Administrativo, por no realizar el seguimiento, a la baja ejecución en las actividades No. 125 a la 134 del plan de acción de la vigencia 2021; correspondientes a la línea de acción "uso y aprovechamiento de las TICS para generar un entorno de gobierno digital confiable y seguro" en el plan cuatrienal de acción.
ACCIÓN PROPUESTA. Efectuar seguimiento al avance de ejecución de las actividades planeadas para cumplir los logros estratégicos asociados a las TIC, en el marco del equipo técnico de Seguridad de la Información (Res. 428-2021); y presentar los resultados con posibles rutas de acción para la toma de decisiones del Equipo Directivo, en las sesiones del CIGD en las que se presente seguimiento al plan de acción institucional, a fin de procurar el cumplimiento efectivo de las metas del cuatrienio relacionadas.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. Se consultó los soportes en la ruta Q:\12_SSI\Evidencias PAA 2023\Evidencias 2023, de acuerdo a memorando 2023IE11731 remitido a la Oficina de Control Interno, en el cual indican: "*Para este hallazgo de Auditoría externa y que hace referencia a diez (10) actividades indicadas en este plan de acción 2020 (numeral 125 al 134) y cuya dependencia responsable de la ejecución es la Dirección Administrativa (componentes de sistemas), SSI a la fecha ha creado una ruta en la red donde se centralizará todas las evidencias o actividades gestionadas para cumplir con los compromisos indicados ("Método de verificación" y la "Programación") y de esta forma documentar y atender principalmente las seis (6) labores que no tienen ningún avance de gestión. Así mismo, se registrará todo el desarrollo de ejecución de las otras labores establecidas en este Plan.* *Como avance de resultados a las anteriores actividades, SSI puede indicar lo siguiente:* *1. Se presentaron reuniones virtuales dirigidas a la identificación de los principios de políticas de gobierno digital y seguridad, así como capacitaciones y evaluaciones de ITIL V4.* *2. Evaluaciones de efectividad de controles - ISO27001:2013 y el MSPI (modelo de seguridad y privacidad de la información)* *3. Seguimiento a la ejecución de los planes de mejora delas auditorías realizadas a los procesos SSI.* *4. Se llevan a cabo monitoreos a los riesgos de seguridad de la información.* *5. Se está documentando las necesidades de contratación, con el fin de contar con mano de obra calificada y necesaria que requiere la SSI.* *6. La SSI cuenta con el informe final del contrato 200224 que consiste en la implementación del protocolo IPv6.*" Consultados los soportes, se observa: - Actividad 125 de 2021: Realizar las actividades requeridas para la solicitud de los procesos de contratación (Togaf, COBIT, ITIL). Para esta actividad, se observa avance en ITIL, no hay soportes sobre TOGAF y COBIT.

- Actividad 126 de 2021: Revisar el cumplimiento de las políticas y procedimientos de seguridad de la información en la Corporación.
En las evidencias se observan dos documentos en Excel “Autodiagnóstico política de Gobierno digital 2023-I” y “2023. Instrumento_Evaluacion_MSPI”, este último contiene el Instrumento de identificación de la línea base de seguridad, evaluación de efectividad de controles - ISO 27001:2013 Anexo a, avance ciclo de funcionamiento del modelo de operación (PHVA), nivel de madurez modelo seguridad y privacidad de la información y calificación frente a mejores prácticas en ciberseguridad (NIST), con fecha de evaluación 21/04/2023; documentos que permiten comprobar el seguimiento avance de la acción.

- Actividad 127 de 2021: Efectuar seguimiento al cumplimiento de los planes de mejora y acciones correctivas de las auditorías realizadas al proceso SSI.
Esta actividad en la evaluación realizada por la OCI, si bien no se cumplió al 100%, tampoco presento baja ejecución en la vigencia, sin embargo, se evidencia avance relacionado con el seguimiento a los planes de mejoramiento durante los dos primeros trimestres de 2023.

- Actividad 128 de 2021: Efectuar monitoreo a la gestión de riesgos de seguridad de la información de la Corporación.
En el mismo sentido de la actividad 127, no se cumplió al 100%, tampoco presento baja ejecución en la vigencia.

- Actividad 129 de 2021: Fortalecer el conocimiento en temas de seguridad de la información.
Consultados los soportes, se observa que durante los dos primeros trimestres de 2023, el proceso SSI ha realizado charlas sobre ciberseguridad con representantes de FORTINET, desde la cuenta de correo seguridadinformacion@concejobogota.gov.co, envían permanentemente pautas informativas CIBERLUNES DE SEGURIDAD, lo que evidencia seguimiento y avance de la acción.

- Actividad 130 de 2021: Realizar un análisis de vulnerabilidades en seguridad de la información.
En la ruta Q:\12_SSI\Evidencias PAA 2023\Actividades 2023\130, no se evidencias archivos que soporten avance a la acción.

- Actividad 131 de 2021: Establecer los parámetros para la visualización de información en la sede electrónica.
En la ruta de la carpeta Q:\12_SSI\Evidencias PAA 2023\Actividades 2023\131, no hay documentos que evidencien avances de la acción.

- Actividad 132 de 2021: Realizar las actividades requeridas para la solicitud de los procesos de contratación, para infraestructura tecnológica (hardware y software).
Consultados los soportes, se observa que durante la vigencia 2022, el proceso SSI en cabeza de la Dirección Administrativa, gestionó los siguientes contratos: Solicitud de contratación 22 mayo 2022, producto de esta gestión se suscribió el contrato 220900, Objeto: Contratar la suscripción, soporte y actualización de productos Adobe y CorelDraw e instalación funcional para el Concejo de Bogotá. Solicitud de contratación 18 julio 2022, producto de esta gestión se suscribió el contrato 220445, objeto: Implementar una solución tecnológica integral de interconexión para el nuevo edificio del Concejo de Bogotá D.C. Solicitud de contratación 27 julio 22, producto de esta gestión se suscribieron los siguientes contratos: Contrato 220773, Adquirir equipos de tecnología y periféricos para el Concejo de Bogotá D.C., Contrato 220774, Adquirir equipos de tecnología y periféricos para el Concejo de Bogotá D.C., Contrato 220775, Adquirir equipos de tecnología y periféricos para el Concejo de Bogotá D.C., Contrato 220885, Objeto: Adquisición de cámara y accesorios fotográficos para el Concejo de Bogotá. Solicitud de contratación formato GFI-FO-007

sin fecha, producto de esta gestión se suscribió Contrato 220674, Adquirir licencias de Office y Windows Server para el Concejo de Bogotá D.C.
En la vigencia 2023, presentan solicitud de contratación con fecha junio de 2023, cuyo objeto es: "Realizar la consultoría para los diagnósticos, estudios y diseños necesarios, para la modernización y optimización de los edificios e instalaciones del Concejo de Bogotá", documento sin firma.
Por lo anterior, se confirma cumplimiento a la ejecución de la acción durante la vigencia 2022.

- Actividad 133 de 2021: Finalizar la implementación del protocolo IPV6 en el Concejo de Bogotá. Luego de verificar las carpetas compartidas con los soportes del Proceso de Sistemas y Seguridad de la Información, ruta ADMINSITRATIVA (\\CBPRINT) Q:\12_SSI\Plan de acción 2021\133 se observa que existe el documento "Informe Final contrato 200224.pdf", dentro del cual en el punto 5, Realizar las Fases 1, 2 y 3 de la "Guía de transición de IPv4 a IPv6 para Colombia" dada por MinTIC, de conformidad con lo establecido en el documento ficha técnica, referencian carpeta compartida en drive https://drive.google.com/drive/folders/1dECg5EA6sqZ8HXeb4y32AcCJYSqFYN2M, en la cual se encuentra el documento "Informe de Implementación IPv6.pdf", en este documento se listan todas las configuraciones realizadas con el protocolo IPv6 dentro de la infraestructura tecnológica del CONCEJO DE BOGOTÁ; es decir, esta actividad se cumplió.

- Actividad 134 de 2021: Establecer la infraestructura crítica de tecnología.
Esta actividad está asociada al logro 53 del cuatrienio "Plan de recuperación de desastres de tecnología adoptado", el cual presentó modificación en el plan indicativo, inicialmente tenía la siguiente programación: vigencia 2021 con 0,5 y 2022 con 0,5; con la modificación se reprogramó el rezago para la vigencia 2023 con 0,5. Para la vigencia 2022 se cumplió con lo programado y, la vigencia 2023 se encuentra en ejecución de acuerdo a la reprogramación.

No se evidencian soportes de reuniones con el Equipo Técnico de Seguridad de la Información y con el CIGD, en el cual se traten los temas relacionados con la No conformidad, con el fin de presentar los resultados con posibles rutas de acción para la toma de decisiones del Equipo Directivo, de acuerdo al plan de mejoramiento suscrito por el proceso SSI.

CONCLUSION. En conclusión y, luego de verificar los soportes, se otorga con un avance del 70% de cumplimiento de la acción. En ejecución.

IX. SEGUIMIENTO MATRIZ DE RIESGOS Y ANÁLISIS DE CONTROLES

RIESGOS DE GESTIÓN

Riesgo No. 1	**Posibilidad de afectación reputacional por afectación en la prestación de los servicios tecnológicos, debido a una inadecuada configuración de la infraestructura tecnológica de la Corporación**
Clasificación de riesgo	Ejecución y Administración de procesos
Causa	1. Inmediata: Indisponibilidad de las aplicaciones o sistemas de información que afecta la gestión rutinaria de los diferentes procesos de la Corporación. 2. Raíz: Desconocimiento en el manejo de las herramientas del proceso.

	3. Raíz: No contar con el debido soporte del fabricante de los componentes de la infraestructura tecnológica o de su representante en el país.
Impacto	1. El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Actividad de control	1. Los profesionales del proceso de Sistemas, validan permanentemente el soporte con los fabricantes o los representantes en el país de las herramientas tecnológicas. 2. El equipo de Sistemas y Seguridad de la Información, verifica que los proveedores o fabricantes realicen la transferencia de conocimiento a los funcionarios de sobre el manejo de las herramientas, dependiendo de las necesidades. De no hacerse en los tiempos requeridos se solicita mediante comunicación el cumplimiento de los compromisos para no afectar la operación de la Corporación.
Plan de tratamiento de riesgos	No se define plan de tratamiento dado que el riesgo residual se encuentra en nivel bajo.
Actividad	No se define plan de tratamiento dado que el riesgo residual se encuentra en nivel bajo.
Tiempo	No se define plan de tratamiento dado que el riesgo residual se encuentra en nivel bajo.

EVALUACIÓN DEL RIESGO

Criterio	Calificación PROCESO	Observación
¿La identificación del riesgo es adecuada frente a lo dispuesto en la guía de administración de riesgos?	Si	La Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5 de la Función Pública recomienda iniciar la redacción del riesgo, como posibilidad de… y luego incluir el Impacto, la Causa inmediata y la Causa raíz.
¿Existe una debida alineación entre el evento, la causa y el Impacto o consecuencia?	Si	La redacción del riesgo incluye las causas y el impacto.
¿Los controles diseñados cubren la causa del riesgo?	Si	Los profesionales del proceso SSI validan el soporte con los fabricantes de las herramientas tecnológicas y solicitan trasferencia de conocimiento a los servidores de la Corporación sobre el manejo de las herramientas.

EVALUACIÓN DEL DISEÑO DEL CONTROL

Criterio	Calificación PROCESO	Observación OCI
¿Existe un responsable asignado a la ejecución del control?	Asignado	Si, los profesionales del proceso SSI.
¿El responsable tiene la autoridad y adecuada segregación de	Adecuado	Si, los profesionales del proceso solicitan a los proveedores y

funciones en la ejecución del control?		fabricantes el soporte y transferencia de conocimiento.
¿El control tiene una periodicidad definida para su ejecución?	Se requiere ajuste	A pesar de ser manual el control, se ejecutan sin una periodicidad definida. Se recomienda establecer una periodicidad para la ejecución de los controles.
¿El control tiene un propósito que indique para qué se realiza? (verificar, validar, conciliar, comparar, revisar, cotejar)	Prevenir	Si, el objeto de los controles es verificar y validar el cumplimiento de soporte y transferencia de conocimiento con los proveedores y fabricantes.
¿Se establece el cómo se realiza la actividad de control?	Se requiere ajuste	Los controles no establecen como se realizan las actividades de control.
¿Se establece qué pasa con las observaciones o desviaciones resultantes de ejecutar el control?	Se corrige	Si, se solicita mediante comunicación a los proveedores o fabricantes el cumplimiento de los compromisos para no afectar la operación de la Corporación.
¿Existe evidencia de la ejecución del control?	Adecuado	Si, videos, grabaciones y actas de asistencia a capacitaciones o sesiones de transferencia de conocimiento sobre los bienes o servicios adquiridos.

VERIFICACIÓN DE PLANES DE TRATAMIENTO

Criterio	Calificación PROCESO	Observación OCI
¿Para los controles débiles y moderados, se evidencia formulación y ejecución del plan de tratamiento? Describa los resultados	No	No se define plan de tratamiento, dado que el riesgo residual se encuentra en nivel bajo.

Riesgo No. 2	**Posibilidad de afectación reputacional por obsolescencia de la infraestructura tecnológica de la Corporación, debido a incumplimiento en los alcances de las metras establecidas en el PETI.**
Clasificación de riesgo	Fallas Tecnológicas
Causa	1. Inmediata: Obsolescencia tecnológica y vulnerabilidades no solucionadas, accesos no autorizados y dificultad para la adopción de las políticas de Seguridad y Privacidad de la Información 2. Inmediata: Inadecuada gestión de copias de seguridad y deficiencias en almacenamiento de información 3. Raíz: Aparición de nuevas tecnologías 4. Raíz: Desaparición o fusión de fabricantes 5. Raíz: No culminar adecuadamente los procesos de contratación 6. Raíz : Insuficiencia de recursos para la actualización tecnológica

Impacto	1. El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores
Actividad de control	1. El equipo de Sistemas y Seguridad de la Información, verifica de forma regular las necesidades de actualización de los sistemas, de acuerdo a los requerimientos y realiza la gestión para hacer las solicitudes de recursos que permitan contar con las inversiones requeridas. Las solicitudes se consolidan en las correspondientes fichas técnicas y solicitudes de contratación. 2. Los profesionales del proceso de Sistemas y Seguridad de la Información de acuerdo al cronograma de contratación, verifican y gestionan los contratos de soporte para la actualización o renovación de la infraestructura tecnológica. Las solicitudes se diligencian en las fichas técnicas y solicitudes de contratación.
Plan de tratamiento de riesgos	No se define plan de tratamiento dado que el riesgo residual se encuentra en nivel bajo.
Actividad	No se define plan de tratamiento dado que el riesgo residual se encuentra en nivel bajo.
Tiempo	No se define plan de tratamiento dado que el riesgo residual se encuentra en nivel bajo.

EVALUACIÓN DEL RIESGO

Criterio	Calificación PROCESO	Observación
¿La identificación del riesgo es adecuada frente a lo dispuesto en la guía de administración de riesgos?	Si	La Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 5 de la Función Pública recomienda iniciar la redacción del riesgo, como posibilidad de… y luego incluir el Impacto, la Causa inmediata y la Causa raíz.
¿Existe una debida alineación entre el evento, la causa y el Impacto o consecuencia?	Si	La redacción del riesgo incluye las causas y el impacto.
¿Los controles diseñados cubren la causa del riesgo?	No	Los profesionales de SSI verifican las necesidades de actualización de los sistemas y realizan la gestión para hacer las solicitudes de los recursos, en el mismo sentido, verifican y gestionan los contratos de soporte para la actualización o renovación de la infraestructura tecnológica.

EVALUACIÓN DEL DISEÑO DEL CONTROL

Criterio	Calificación PROCESO	Observación OCI
¿Existe un responsable asignado a la ejecución del control?	Asignado	Si, los profesionales del proceso SSI.
¿El responsable tiene la autoridad y adecuada segregación de	Adecuado	Si, los profesionales del proceso realizan la gestión para hacer las

funciones en la ejecución del control?		solicitudes de recursos y gestionan los contratos de soporte para la actualización o renovación de la infraestructura tecnológica.
¿El control tiene una periodicidad definida para su ejecución?	Se requiere ajuste	A pesar de ser manual el control, se ejecutan sin una periodicidad definida. Se recomienda establecer una periodicidad para la ejecución de los controles.
¿El control tiene un propósito que indique para qué se realiza? (verificar, validar, conciliar, comparar, revisar, cotejar)	Prevenir	Si, el objeto de los controles es verificar las necesidades de actualización de los sistemas y verificar y gestionar los contratos.
¿Se establece el cómo se realiza la actividad de control?	Se requiere ajuste	Los controles no establecen como se realizan las actividades de control.
¿Se establece qué pasa con las observaciones o desviaciones resultantes de ejecutar el control?	Incompleto	No, se recomienda establecer que sucede con las observaciones o desviaciones resultantes de ejecutar los controles.
¿Existe evidencia de la ejecución del control?	Adecuado	Si, memorando de solicitud de necesidades, fichas técnicas, solicitudes de contratación.

VERIFICACIÓN DE PLANES DE TRATAMIENTO

Criterio	Calificación PROCESO	Observación OCI
¿Para los controles débiles y moderados, se evidencia formulación y ejecución del plan de tratamiento? Describa los resultados	No	No se define plan de tratamiento, dado que el riesgo residual se encuentra en nivel bajo.

RIESGOS DE CORRUPCIÓN

Riesgo No. 9	**Posibilidad de recibir dádivas o beneficios en nombre propio y/o de un particular para realizar el acceso indebido, hurto, manipulación o adulteración de la información del Concejo de Bogotá D.C.**
Clasificación de riesgo	Corrupción
Causa	1. Sistemas de Información susceptibles de manipulación o adulteración por personas no autorizadas. 2. Falta de definición e implementación de controles para el acceso a la información.
Impacto	1. Perdida de la información 2. Perdida de la imagen y reputación. 3. Sanciones disciplinarias. 4. Sanciones penales. 5. Sanciones fiscales
Actividad de control	1. El Sistema de copias de seguridad, diariamente genera una copia de respaldo de la información en otro medio, el profesional asignado

	verifica, que se haya realizado correctamente, de encontrarse inconsistencias se detecta la causa y se genera nuevamente el backup. 2. Cada servidor público del Concejo de Bogotá de forma permanente da cumplimiento del Manual de Políticas de seguridad de la información, verifica que hace uso correcto a los sistemas a su cargo. Cuando se presenten fallas solicita la presencia de la mesa de ayuda. En caso de no dar cumplimiento al Manual, se llevan a cabo las acciones disciplinarias a que se dé lugar.
Plan de tratamiento de riesgos. Actividad	Sensibilización o divulgación de lo establecido en el Manual de políticas de seguridad de la información.
Soporte	Evidencias de las actividades realizadas (Correos con las divulgaciones, fotos y registros de asistencias, entre otras)
Tiempo	Diciembre de 2023

EVALUACIÓN DEL RIESGO

Criterio	Calificación PROCESO	Observación
¿La identificación del riesgo es adecuada frente a lo dispuesto en la guía de administración de riesgos?	No	La Guía de Riesgos de la Función Pública recomienda iniciar la redacción del riesgo, como posibilidad de… y luego incluir el Impacto (Las consecuencias que puede ocasionar a la organización la materialización del riesgo), la Causa inmediata (circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo) y la causa raíz (causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo).
¿Existe una debida alineación entre el evento, la causa y el Impacto o consecuencia?	No	No se incluye en la redacción del riesgo las causas y el impacto.
¿Los controles diseñados cubren la causa del riesgo?	Incompleto	Se recomienda incluir controles que cubran las causas planteadas, como la seguridad aplicada a los usuarios, a los equipos, monitoreo de la plataforma tecnológica, etc. El control No. 2 habla de sanciones disciplinarias en caso de no dar cumplimiento al manual, es decir, luego de posiblemente materializado el riesgo.

EVALUACIÓN DEL DISEÑO DEL CONTROL

Criterio	Calificación PROCESO	Observación OCI
¿Existe un responsable asignado a la ejecución del control?	Incompleto	El control No. 1 si tiene funcionario responsable, el profesional encargado de las copias de

		seguridad. El control No. 2 no establece un funcionario asignado.
¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Se requiere ajuste	Al no tener un funcionario asignado para el control No. 2, se recomienda replantear la redacción del control.
¿El control tiene una periodicidad definida para su ejecución?	Incompleto	Para el control No. 1 si, se realiza a diario, para el control No. 2 no.
¿El control tiene un propósito que indique para qué se realiza? (verificar, validar, conciliar, comparar, revisar, cotejar)	No	Se recomienda replantear la redacción de los controles e incluir el propósito.
¿Se establece el cómo se realiza la actividad de control?	Se requiere ajuste	Los controles no establecen como se realizan las actividades de control.
¿Se establece qué pasa con las observaciones o desviaciones resultantes de ejecutar el control?	Adecuado	Si, para el control No. 1, de encontrarse inconsistencias se detecta la causa y se genera nuevamente el backup. Para el control No. 2, En caso de no dar cumplimiento al Manual, se llevan a cabo las acciones disciplinarias a que se dé lugar.
¿Existe evidencia de la ejecución del control?	Incompleto	Para el control No. 1 si, formato SSI-PR002-FO1 – Bitacora Backups de forma diaria. Para el control no. 2 no.

VERIFICACIÓN DE PLANES DE TRATAMIENTO

Criterio	Calificación PROCESO	Observación OCI
¿Para los controles débiles y moderados, se evidencia formulación y ejecución del plan de tratamiento? Describa los resultados	Si	Sensibilización o divulgación de lo establecido en el Manual de políticas de seguridad de la información.

Riesgo No. 10	**Posibilidad de recibir una dádiva o beneficio propio y/o de un particular para obstaculizar el acceso a un sistema informático del Concejo de Bogotá D.C.**
Clasificación de riesgo	Corrupción
Causa	1. Acceso indebido a los sistemas. 2. Vulnerabilidades de las plataformas de los sistemas informáticos.
Impacto	1. Perdida de la imagen y reputación. 2. Sanciones disciplinarias. 3. Sanciones penales. 4. Sanciones fiscales.
Actividad de control	El responsable de cada sistema verifica, de forma permanente que los sistemas estén actualizados a la versión más estable del fabricante o

	proveedor. En caso de no poder actualizar los sistemas se aplican controles alternos.
Plan de tratamiento de riesgos. Actividad	Realizar monitoreo de los sistemas de información.
Soporte	Reporte generado por la plataforma de monitoreo.
Tiempo	Diciembre de 2023.

EVALUACIÓN DEL RIESGO

Criterio	Calificación PROCESO	Observación
¿La identificación del riesgo es adecuada frente a lo dispuesto en la guía de administración de riesgos?	No	La Guía de Riesgos de la Función Pública recomienda iniciar la redacción del riesgo, como posibilidad de… y luego incluir el Impacto (Las consecuencias que puede ocasionar a la organización la materialización del riesgo), la Causa inmediata (circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo) y la causa raíz (causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo).
¿Existe una debida alineación entre el evento, la causa y el Impacto o consecuencia?	No	No se incluye en la redacción del riesgo las causas y el impacto.
¿Los controles diseñados cubren la causa del riesgo?	Si	El responsable de cada sistema verifica, de forma permanente que los sistemas estén actualizados a la versión más estable del fabricante o proveedor. En caso de no poder actualizar los sistemas se aplican controles alternos (restringiendo el acceso a nivel de firewall y respaldar la información con sistema Hiperconvergente).

EVALUACIÓN DEL DISEÑO DEL CONTROL

Criterio	Calificación PROCESO	Observación OCI
¿Existe un responsable asignado a la ejecución del control?	Corregir	Se recomienda nombrar los sistemas y asignar responsable.
¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Se requiere ajuste	Al no tener un funcionario asignado para el control, se recomienda replantear la redacción del control.
¿El control tiene una periodicidad definida para su ejecución?	Incompleto	Se recomienda incluir la periodicidad de la actividad de control.
¿El control tiene un propósito que indique para qué se realiza?	No	Se recomienda replantear la redacción del control e incluir el propósito.

(verificar, validar, conciliar, comparar, revisar, cotejar)		
¿Se establece el cómo se realiza la actividad de control?	Se requiere ajuste	Los controles no establecen como se realizan las actividades de control.
¿Se establece qué pasa con las observaciones o desviaciones resultantes de ejecutar el control?	Adecuado	Si, en caso de no poder actualizar los sistemas se aplican controles alternos (restringiendo el acceso a nivel de firewall y respaldar la información con sistema Hiperconvergente).
¿Existe evidencia de la ejecución del control?	No	No, en el formato SSI-PR001- FO1 no se evidencia ejecución del control, la mayoría de eventos es relacionada con verificación física del estado de la infraestructura.

VERIFICACIÓN DE PLANES DE TRATAMIENTO

Criterio	Calificación PROCESO	Observación OCI
¿Para los controles débiles y moderados, se evidencia formulación y ejecución del plan de tratamiento? Describa los resultados	Si	Realizar monitoreo de los sistemas de información. El proceso cuenta con las siguientes herramientas: FortiSIEM, Consola Oracle Cloud, StruxureWare Data Center Expert y Consola VMware, desde las cuales se realiza monitoreo al estado de los servidores y gestión de la capacidad, monitoreo a las Bases de Datos, a los cluster del sistema de hiperconvergencia y a los aires acondicionados y UPS.

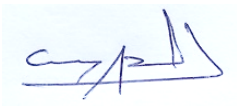
RECOMENDACIONES.

- Se recomienda que la Corporación establezca acciones que permitan contar con un Oficial de Seguridad de la Información de manera permanente, dado los inconvenientes y atrasos presentados en los temas asociados a la implementación de la Política de Gobierno Digital y Seguridad Digital, actividades que de acuerdo al Manual de Roles y Responsabilidades vigente en la Corporación, están a cargo del Oficial de Seguridad de la Información.
- Se recomienda que los responsables prioricen las necesidades de contratación relacionadas al proceso de Sistemas y Seguridad de la Información, puesto que las líneas de contratación de las actividades 66, 112 y 113 para la vigencia 2022, fueron desfinanciadas de acuerdo al Memorando 2022IE16573, estas mismas fueron incluidas en el plan de acción anual vigencia 2023 (Actividades 80, 140 y 141) sin presentar modificaciones, lo que hace que presenten riesgo de no cumplimiento a los logros y metas institucionales del componente de Tecnologías de la Información y las Comunicaciones.
- Se recomienda tener en cuenta la guía para la administración de riesgos adoptada en la corporación, con el propósito de verificar las observaciones plasmadas en el presente informe de auditoría numeral “IX. Seguimiento Matriz de Riesgos y Análisis de Controles” para los

riesgos de gestión, de corrupción y de seguridad digital, en lo concerniente con la redacción y establecimiento de controles.
- Se recomienda que el proceso tenga en cuenta las oportunidades de mejora comunicadas en el presente informe, los cuales contribuyen en la mejora continua de los procedimientos.
- Finalmente, se reitera la importancia de finalizar la actualización de los procedimientos y documentos del proceso, así como el inventario de activos de información con el propósito de darle cierre a las acciones abiertas en los planes de mejoramiento.

CONCLUSIONES.

- Se evidencia compromiso del Proceso Sistemas y Seguridad de la información con los Planes de mejoramiento derivados de auditorías anteriores, sin embargo, al no contar con un Responsable de Seguridad de la Información de manera permanente, dificulta y retrasa el cumplimiento de las acciones propuestas en los mismos, así como los logros y metas del plan de acción cuatrienal y en la implementación de la Política de Gobierno y Seguridad Digital.
- Las No conformidades comunicadas en el presente informe son producto de falencias en la actualización de algunos documentos que soportan el proceso y otras que se derivan del cumplimiento de responsabilidades.

AUDITOR LÍDER	
Nombre: CARLOS ANDRES PADILLA PINTO	Firma: 
EQUIPO AUDITOR	
Nombre (s): JOSÉ GABRIEL PARRA PIRAZAN	Firma (s): 

JEFE OFICINA DE CONTROL INTERNO	
Nombre: JEIMMY CAROLINA RUEDA CASTILLO	Firma: Firmado digitalmente por Jeimmy Carolina Rueda Castillo

FECHA DE ENTREGA	30 de octubre de 2023