Proceso:	Sistemas y Seguridad de la Información
Líder del proceso/Jefe de dependencia:	Director Administrativo
Objeto:	Implementar, administrar, renovar, mantener y soportar la infraestructura tecnológica y el Sistema de Seguridad de la Información del Concejo, mediante la gestión y operación de los mismos para fortalecer la gestión institucional.
Alcance:	Cubre la verificación de las actividades establecidas en los procedimientos seleccionados (Plan de Necesidades de Contratación y Seguimiento; Gestión de Activos; Clasificación, Etiquetado y Manejo de Información; Gestión Incidentes Seguridad información; Gestión de la Capacidad; Atención de Soporte Tecnológico y Continuidad del Negocio) en relación con el plan de acción, indicadores, la contratación y la gestión de riesgos. Adicionalmente, se comprobará el cumplimiento del plan de mejoramiento. Es importante recalcar que el desarrollo de la presente auditoría interna presenta el limitante que debido al confinamiento derivado del Covid 19, se realizó con base en lo publicado por el Proceso y la Corporación en las carpetas internas, la página Web y soportes que logró facilitar el Líder del Proceso.
Criterios:	- Constitución Política de Colombia - 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 y se dictan otras disposiciones*". - 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. - Decreto 1072 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo*" y sus reglamentarios. - Resolución 634 de 2014 Organigrama - Resolución 635 de 2014 Normograma - Resolución 1007 de 2015 "Mapa de Procesos" - Resolución 720 de 2013 "*Por la cual se aprueba el Manual de Procesos y Procedimientos del Concejo de Bogotá D.C.*" - Resolución 1053 de 2015 "*Por medio de la cual se adopta el Manual de Políticas de Operación para el Concejo de Bogotá D.C.*"

	- Resolución 514 de 2015 Manual de Funciones y Competencias Laborales y sus modificatorias - Resolución 0486 de 2016 "*Por la cual se adopta el Plan de Acción Cuatrienal del Concejo de Bogotá D.C., para el período constitucional 2016-2019*" - Resolución 529 de 2018 "*Por la cual se aprueba la modificación al Plan de Acción Cuatrienal 2016-2019 y la modificación al Plan de Acción del Concejo de Bogotá, para la vigencia 2018*" - Resolución 091 de 2020 "*Por medio de la cual se adopta el Plan de Acción para la vigencia 2020*" - Resolución 822 de 2019 "*Por medio de la cual se adopta la Política de Administración del Riesgo en el Concejo de Bogotá D.C., para la vigencia 2019*" - Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP 2018. - Guía para la construcción y análisis de indicadores de gestión DAFP 2018 - Norma Técnica NTC 5854 5854 de 2011 Accesibilidad a páginas web - Directiva 002 de 2018 Tratamiento de datos personales. - Manual de Gobierno Digital - Guía para la elaboración del Plan de Seguridad y Privacidad de la Información - CONPES 3854 de 2016 Por la cual se define la Política Nacional de Seguridad Digital. - CONPES 3701 de 2011 Lineamientos de política para ciberseguridad y ciberdefensa. - Modelo Nacional de Gestión de Riesgos de Seguridad Digital - Resolución 305 de 2008 - Alcaldía Mayor "*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 "*Por la cual se modifica la Resolución 305 de 2008 de la Comisión Distrital de Sistemas*". - Decreto 1008 de 2018 "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*". - Planes de Mejoramiento Demás Normas que les apliquen.

Equipo Auditor:	Nidia Cano Sánchez (Auditor Líder).	
Auditados:	Daniel Andrés García Cañón - Director Administrativo Francisco Javier Bernal García – Líder Operativo del Proceso SSI	
Metodología:	• Revisión de la documentación publicada en la Web, intranet y red interna, que soporta el proceso. • Formulación de cuestionarios, respondidos por el responsable del Proceso SSI • Seguimiento a Planes de Mejoramiento. • Seguimiento a Matrices de Riesgos	
Fechas de Ejecución de la Auditoría:	Desde (día/mes/año):	30/04/2020
	Hasta (día/mes/año):	25/06/2020
Reunión de Cierre:	(día/mes/año)	25/06/2020

I. PROCESO DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

1 CONFORMIDADES

1.1 De acuerdo con la muestra se estableció el cumplimiento del Procedimiento de Gestión de Incidentes de Seguridad de la Información respecto a la documentación de los incidentes ocurridos en el segundo semestre de 2019.

1.2 Se estableció que el Proceso de SSI tramita los formatos Relación Elaboración y Seguimiento Fichas Técnicas (SSI-PR005-F05) y Relación y Seguimiento de Contratos (SSI-PR005-F03) en cumplimiento del Procedimiento Plan de Necesidades de Contratación y Seguimiento - SSI-PR005.

1.3 Se determinó el diligenciamiento de las 19 preguntas correspondientes a los Criterios parar calificar el impacto de Riesgos de Corrupción

1.4 En la contingencia actual derivada de la Pandemia del Covid -19 el Proceso de Sistemas y Seguridad de la Información ha contribuido con el acceso al correo institucional y al escritorio de los computadores de la entidad para facilitar el trabajo remoto de los servidores de la Corporación.

2 NO CONFORMIDADES

2.1. Se evidenció que el Proceso de Sistemas y Seguridad de la Información definió en el Plan de Acción de la vigencia 2020 versión 2, cuatro (4) acciones relacionadas con desarrollar las actividades para solicitar la contratación de diferentes productos y servicios a cargo del Proceso;

como: "*Realizar las actividades requeridas para la solicitud de contratación para realizar la implementación del protocolo de internet versión 6 (IPv6)*".
Acciones que hacen referencia al desarrollo del procedimiento para la solicitud de contratación de bienes o servicios; no obstante, se deben reformular en una sola actividad y su medición se efectuará a través de un indicador de eficacia que señale la cantidad programada en el plan anual de adquisiciones de las solicitudes a realizar en el año y si es posible un indicador de eficiencia que permita medir cuántas de esas solicitudes se reflejan en contratos suscritos, para determinar las debilidades y reorientar la gestión.
En consecuencia, no se relacionan la totalidad de las tareas que desarrolla el Proceso y se distorsiona la medición de su desempeño.

Hecho que incumple lo establecido en los literales d. "*Garantizar la correcta evaluación y seguimiento de la gestión organizacional*" y g. "*Garantizar que el Sistema de Control Interno disponga de sus propios mecanismos de verificación y evaluación*" del artículo 2º Objetivos del Sistema de Control Interno de la ley 87 de 1993 y lo definido en el numeral 4.2.1 Seguimiento y Evaluación del Desempeño Institucional del Manual Operativo del Modelo Integrado de Planeación y Gestión versión 3 de diciembre de 2019.

Una vez analizada la respuesta del Proceso concerniente a "…la contratación no es del alcance de este proceso no es posible colocarla como una meta del mismo, el alcance del proceso y de la Dirección Administrativa llega hasta la presentación de la solicitud de contratación ante el Fondo Cuenta…" se observa que no está direccionada a desvirtuar el fundamento de la No Conformidad relacionada con reformular en una sola actividad las cuatro actividades desagregadas que presenta en el Plan de Acción sobre la solicitud de contratación y por ende realizar su medición con indicadores de eficacia y eficiencia , sino que se enfocó a la sugerencia de establecer el indicador de eficiencia.
Por lo tanto, no se acepta la réplica a esta No Conformidad y se ratifica para ser incluida en el Plan de Mejoramiento.

2.2 En el Comité Institucional de Gestión y Desempeño realizado el 27 de febrero de 2020 se estableció que se debían reactivar los Equipos Técnicos creados por la Resolución 388 de 2019 para que estudiaran los planes de su competencia establecidos en la Resolución 612 de 2018. Sin embargo, se evidenció que el Equipo Técnico de Seguridad de la Información no se ha reunido en lo corrido del año para revisar el Plan Estratégico de Tecnologías de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información; los cuales luego serán presentados en el Comité Institucional de Gestión y Desempeño para su aprobación.
Situación que genera demoras en el establecimiento de los planes guía para el desarrollo de las diferentes dimensiones del MIPG.

Lo anterior, incumplió el capítulo 3 Equipos Técnicos de Gestión y Desempeño Institucional de la Resolución 388 de 2019; el literal e. *"Asegurar la oportunidad y confiabilidad de la información y de sus registros*" del artículo 2º Objetivos del Sistema de Control Interno de la ley 87 de 1993, así

como, los numerales 3.2.1.3 Política Gobierno Digital y 3.2.1.4 Política de Seguridad Digital del Manual Operativo del Modelo Integrado de Planeación y Gestión versión 3 de diciembre de 2019.

De la respuesta a esta No Conformidad se destaca: "…*El proceso generó los planes y estos fueron copiados por correo electrónico a la Dirección Administrativa para su respectivo tramite*…"
Sin embargo, se verificó que estos archivos fueron copiados a la Directora Administrativa para su revisión y aprobación.
Adicionalmente, en el acta No. 2 del CIGD se consignó que los planes institucionales debían ser revisados en los Equipos Técnicos competentes para cada caso y luego ser presentados para aprobación en el Comité Institucional de Gestión y Desempeño. Por lo tanto, se decidió modificar la redacción de esta No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.3. Se observó que en la versión 2 del Plan de Acción que fue aprobada en el Comité de Gestión y Desempeño realizado el 14 de mayo de 2020, se ajustaron las actividades a cargo del Proceso de Sistemas y Seguridad de la Información y adicionaron las siguientes: "Revisar el cumplimiento de políticas y/o procedimientos de seguridad de la información en la Corporación, Efectuar seguimiento al cumplimiento de los planes de mejora y acciones correctivas de las auditorías realizadas al SGSI, Realizar prueba de continuidad de los servicios tecnológicos del Concejo de Bogotá, Efectuar monitoreo a la gestión de riesgos de seguridad de la información de la Corporación, Sensibilizar a los servidores públicos de la Corporación en temas de seguridad de la información" las cuales no presentan fecha de inicio ni terminación.

En consecuencia, se dificulta el monitoreo y verificación del avance de las actividades y de su cumplimiento.
Hecho que incumple los literales d. "*Garantizar la correcta evaluación y seguimiento de la gestión organizacional*" y g. "*Garantizar que el Sistema de Control Interno disponga de sus propios mecanismos de verificación y evaluación*" del artículo 2º Objetivos del Sistema de Control Interno de la ley 87 de 1993.
Además, se vulneró el numeral 4.2.1 Seguimiento y Evaluación del Desempeño Institucional del Manual Operativo del Modelo Integrado de Planeación y Gestión versión 3 de diciembre de 2019.

De acuerdo con la respuesta emitida por el Proceso relacionada con "*Se realizará el ajuste en el documento y se tramitará ante la Oficina Asesora de Planeación para su actualización*" se ratifica la No Conformidad y por ende, se debe formular el respectivo plan de mejoramiento.

2.4. Se determinaron las siguientes falencias en la aplicación del Procedimiento Continuidad de Negocio del Subsistema de Seguridad de la Información:
- La Corporación no posee un Plan de Continuidad del Negocio sólo presenta un Plan de Contingencia que solo está enfocada al tema tecnológico.
-No se tienen identificados los procesos críticos
-No se han identificado los factores de riesgo de interrupción sobre los procesos críticos de la Corporación.
-No se encuentran documentados los recursos mínimos de TI

-No se han determinado las estrategias de recuperación tecnológica
-No se realizaron sensibilizaciones de los roles, responsabilidades y acciones a ejecutar
-No se realizó la prueba del plan de contingencia
Por ende, no se ha estructurado un Plan de Continuidad del Negocio con los parámetros definidos en el procedimiento vigente.

Situación que incumplió los numerales 6.1, 6.2, 6.3, 6.4, 6.5, 6.6 y 6.7 establecidos en el Procedimiento Continuidad de Negocio del Subsistema de Seguridad de la Información. Así como, el numeral 3.2.1.3 Política Gobierno Digital del Manual Operativo del Modelo Integrado de Planeación y Gestión versión 3 de diciembre de 2019.

De la objeción del Proceso se destaca lo siguiente: *"…En este sentido se han realizado actividades con los proveedores en el marco de los contratos con el fin de garantizar la alta disponibilidad de los sistemas …*" pese a lo argumentado se ratifica la No Conformidad porque no se cumple con el procedimiento en mención como se detalló en las respuestas dadas a la lista de chequeo enviada por la Oficina de Control Interno. Por ende, se debe formular el plan de mejoramiento respectivo.

2.5 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.

Hecho que incumplió el numeral 6.10 Registrar las Lecciones Aprendidas del Procedimiento de Gestión de Incidentes de Seguridad de la Información SSI-PR007 versión 3 de julio de 2018. Así como, se vulneró el literal f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos*" del artículo 2º Objetivos del Sistema de Control Interno de la ley 87 de 1993.

Se resalta de la respuesta a la No Conformidad lo siguiente: "*…Dado que ninguno de los incidentes se consideró de alta gravedad se determinó continuar con los procesos de socialización y sensibilización de los usuarios …"* Si bien es cierto, los incidentes reportados no son graves, el procedimiento contempla que se deben registrar las lecciones aprendidas en el software de mesa de ayuda y de acuerdo con lo contestado a la pregunta 25 de la lista de chequeo relacionada con el tema *"…las lecciones aprendidas no han sido documentadas dado que el software de mesa de*

ayuda se encuentra en etapa de afinamiento", por lo tanto, el sistema debe estar dispuesto para cumplir con esta actividad.
En consecuencia, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.6 Al revisar el Manual de Políticas de Seguridad de la Información se evidenció que se encuentra desactualizado, entre otras razones, porque hace referencia a Comités que ya fueron eliminados con la entrada en vigor del Modelo Integrado de Planeación y Gestión, como se describe en el numeral 8.2.1.2 relacionado con "*El Oficial de Seguridad de la Información (OSI), … y reportar al Comité Técnico de Seguridad de la Información (CTSI) y al Comité del SIG, el estado de la implementación y seguimiento del SGSI*"
Situación que se repite en el numeral 8.1.1 *"…Estos documentos deben ser revisados por la Alta Dirección con el apoyo del Comité Técnico de Seguridad de la Información…"*
Por lo tanto, el Manual no es una fuente confiable para el desarrollo de las actividades de seguridad de la información.

Situación que incumplió lo establecido en el artículo 6º Creación del Comité Institucional de Gestión y Desempeño de la Resolución 388 de 2019. Así como, el literal e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*" del artículo 2º de la ley 87 de 1993.

De acuerdo con la respuesta emitida por el proceso relacionada con *"…se preparó una nueva versión del manual de políticas de seguridad de la información el cual se encuentra en borrador*…" se corrobora que efectivamente el Manual de Políticas de Seguridad de la Información se encuentra desactualizado. Por ende, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.7 Se estableció que el Proceso de Sistemas y Seguridad de la Información no elabora Planes Anuales de Mantenimiento de la Infraestructura Tecnológica de la Corporación. En consecuencia, se afecta la disponibilidad del servicio de la mencionada Infraestructura.

Situación que incumplió el numeral 8.8.5 Mantenimiento de Equipos del Manual de Políticas de Seguridad de la Información del Concejo de Bogotá D.C., versión 3 del 18 de mayo de 2018; el literal a. "*Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten*" del artículo 2º de la ley 87 de 1993; el numeral 2.8 Planes de mantenimiento, LI.ST.09 de G.ST.01 Guía del dominio de Servicios Tecnológicos MinTIC. Así como, el numeral 3.2.1.3 Política Gobierno Digital del Manual Operativo del Modelo Integrado de Planeación y Gestión versión 3 de diciembre de 2019.

En la respuesta el Proceso afirma que "…*que el proceso si contempla el mantenimiento de la infraestructura, estos se dejan de forma explícita dentro de la ficha técnica de cada uno de los contratos de soporte y adquisición de infraestructura, en los que se especifica la periodicidad y el alcance de las actividades…*" Sin embargo, la No conformidad está direccionada a la no formulación

de Planes Anuales de Mantenimiento Preventivo y Correctivo de la Infraestructura Tecnológica, porque debe existir un documento donde se programen los elementos sujetos de mantenimiento, tipo de mantenimiento, periodicidad, responsable (técnico, proveedor o contratista), entre otros aspectos, dado que esta labor afecta la disponibilidad del servicio y debe ser planificada.
Adicionalmente, la información del mantenimiento que aparece en la ficha técnica de los contratos debe coincidir con lo programado en el Plan Anual de Mantenimiento.
Por lo tanto, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.8. 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 lineamientos[1] 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.

Hecho que vulnera lo establecido en el literal f. "Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos"; del artículo 2º de la ley 87 de 1993. Además, se incumple lo programado en el plan de actualización de los documentos de la Corporación para el año 2019.

De acuerdo con la respuesta emitida por el proceso relacionada con *"…actualmente ya se encuentra en curso la contratación de cuatro profesionales para apoyar las actividades y así poder realizar la actualización durante el segundo semestre de 2020…*" se corrobora que efectivamente los 13 procedimientos del Proceso de Sistemas y Seguridad de la Información se encuentran desactualizados. Por lo tanto, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.9 Se estableció que en la Guia para el Ejercicio de las Funciones de Supervisión y Obligaciones de la Interventoría versión 10 de la Secretaría Distrital de Hacienda, está definida como una función de la supervisión de carácter administrativo la de "*Publicar en el SECOP los requerimientos o informes que realice*" es decir, que debe publicar las aprobaciones, autorizaciones, requerimientos o informes del supervisor o del interventor, que prueben la ejecución del contrato.

[1] Definir el responsable de llevar a cabo la actividad de control.
Indicar cuál es el propósito del control.
Indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
Tener una periodicidad definida para su ejecución.
Establecer el cómo se realiza la actividad de control.
Establecer las evidencias de la ejecución del control.

Sin embargo, al verificar la información publicada en el SECOP II del Contrato de Prestación de Servicios No.190359-1-2019 con objeto de "*Proveer el servicio integral de gestión de mesa de ayuda y gestión de impresión con suministro de repuestos para el Concejo de Bogotá*" se observó que, pese a que inició su ejecución el 26 de julio de 2019, la sección del aplicativo relacionada con Ejecución del Contrato no presenta diligenciado el porcentaje, facturas del contrato y documentos de ejecución del contrato.

En consecuencia, no se está divulgando ni registrando la información pública que exige la ley para el control social.

Hecho que incumplió los artículos 2.1.1.2.1.7 y 2.1.1.2.1.8 del Decreto 1081 de 2015; artículo 2.2.1.1.1.7.1 Publicidad en el SECOP, del Decreto 1082 de 2015; el artículo 11 literal g) de la 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 y se dictan otras disposiciones*"; los artículos 7° y 8º del Decreto 103 de 2015 "*Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*"; el artículo 2° literales a), b), e) y f) de la ley 87 de 1993, los numerales 4.7.1.6 y 4.7.2.4 del Guia Para el Ejercicio de las Funciones de Supervisión y Obligaciones de la Interventoría de la SDH y la Circular Externa Única del 17 de julio de 2018 de Colombia Compra Eficiente.

En la respuesta el Proceso asevera que: "*Desde … el Proceso de Sistemas y Seguridad de la Información se remiten junto con las facturas los informes de supervisión a la Secretaria Distrital de Hacienda, … y dado que es quien posee los accesos para la administración a la plataforma del SECOP… pero no tiene dentro de su alcance la administración de dicha plataforma de contratación*." Pese a lo anterior, la Oficina de Control Interno resalta que en las normas que regulan la obligación de actualizar el SECOPII no existen excepciones para su desarrollo y el Proceso no anexa los soportes que eximan a los supervisores del Concejo de Bogotá D.C. del cumplimiento legal de este deber.

Adicionalmente, se concluye falta de gestión por parte del Proceso, al no requerir las claves o accesos respectivos para lograr actualizar el SECOPII.
Por lo tanto, se ratifica la No Conformidad y debe ser incluida en el Plan de Mejoramiento.

2.10. Se evidenció que la Política de Administración de Riesgos del Concejo de Bogotá D.C. no señala la decisión de la Corporación de realizar la gestión de riesgos a todos los activos de seguridad digital identificados o sí solo se aplican a los calificados con un mayor nivel de criticidad.

Situación que se originó por debilidades en elaboración de la política de riesgos. Lo que incide en que la Política no incluye todos los aspectos primordiales que apoyan una adecuada gestión de los riesgos y que debieron ser aprobados por el Comité Institucional de Control Interno.

Hecho que incumplió las recomendaciones definidas en el numeral 4.1.6 Identificación de Activos de Seguridad Digital del Anexo 4 Lineamientos para la gestión de riesgos de Seguridad Digital en entidades públicas emitido en el 2018.

En la respuesta el Proceso afirma que: "…*la Política de Administración de Riesgos del Concejo de Bogotá D.C. no es competencia del proceso de Sistemas y Seguridad de la Información, este proceso se limita a acatar lo allí establecido bajo los directrices dadas por la Oficina Asesora de Planeación*" Se aclara que la política de administración de riesgos engloba todas la directrices para la gestión de riesgos, que incluyen los riesgos de seguridad de la información, los cuales requieren un tratamiento especial, por lo tanto, se debe tener un compromiso y co-responsabilidad con la aplicación y mejoramiento de la mencionada política.
Además, el Proceso debe cumplir con las responsabilidades establecidas para la primera línea de defensa[2], especialmente la relacionada con "*Conocer y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo*".
En consecuencia, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.11 Se observó el incumplimiento de las directrices para identificar los riesgos de seguridad digital, respecto a que no se evidenció el establecimiento del contexto externo e interno, ni la actualización del inventario de Activos de la Información, tampoco se realizó el análisis conjunto de activos del mismo tipo, por ejemplo, hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo y no se definieron en forma individual los riesgos por pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos.
Hecho que se generó por falencias en la aplicación de la metodología para la gestión de los riesgos de seguridad digital e incidió en la adecuada identificación de los riesgos.
Situación que incumplió lo establecido e los numerales 4.1.1, 4.1.6 y 4.1.7 del Anexo 4 "*Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas*".
en el numeral 2.2 Identificación de Riesgos (Formato de descripción del riesgo de seguridad digital) de la Guía para la Administración de Riesgos y Definición de Controles en Entidades Públicas.

De acuerdo con la respuesta emitida por el Proceso relacionada con "*Junto con la oficina Asesora de Planeación se revisará la Guía para la Administración de Riesgos y Definición de Controles en Entidades Públicas y se realizaran los ajustes que le correspondan al proceso*" por lo tanto, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.12 Se observó que para el tratamiento de los riesgos de corrupción del Proceso de SSI seleccionó para ambos riesgos la opción de "Evitar", la cual se define como "*Se abandonan las actividades*

[2] Guia de Política de Administración del Riesgo versión 01 del 18 de noviembre de 2019. Pág. 16.

que dan lugar al riesgo y se decide no iniciar o no continuar con las actividades que lo causan". No obstante, se definieron actividades de control en el Plan de Tratamiento, por lo tanto, la opción correcta debió ser "Reducir"
Situación que es producto de falencias en la aplicación de la metodología. En consecuencia, se debe revisar y ajustar el mapa de riesgos.
Hecho que incumplió el acápite de "Tratamiento del riesgo" de la Guía para la Administración de Riesgos y Definición de Controles en Entidades Públicas. Así como, el literal f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos*" del artículo 2º de la ley 87 de 1993.

En la respuesta emitida por el Proceso sugiere que se trate como una oportunidad de mejora "…que el proceso tendrá en cuenta para para las nuevas formulaciones de dichos documentos…" En consideración a que se tomen medidas para no incurrir en errores se decide ratificar la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.13 Si bien es cierto en el ejercicio de la identificación de los riesgos de seguridad digital, el mapa de riesgos del Proceso presenta amenazas y vulnerabilidades no se encontraron los catálogos donde se describan las fuentes que pueden hacer daño a los activos y materializar los riesgos (amenazas) ni el listado de debilidades por tipo (vulnerabilidades), que fueron utilizadas para la administración del riesgo de la vigencia 2020.
Además, estos aspectos no fueron desarrollados en la Política de Riesgos.

Situación que incide en que la Política de Riesgos no contempla todas las directrices necesarias para el desarrollo de la gestión de riesgos de seguridad digital.
Hecho que incumple lo establecido en el numeral 4.1.7 Identificar los Riesgos Inherentes del Anexo 4 "Lineamientos para la Gestión de riesgos de Seguridad Digital en Entidades Públicas" de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" versión 4 de octubre de 2018.

De acuerdo con la respuesta emitida por el proceso relacionada con "*Junto con la oficina Asesora de Planeación se revisará la Guía para la Administración de Riesgos y Definición de Controles en Entidades Públicas y se realizaran los ajustes que le correspondan al proceso*" por lo tanto, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.14 Se observó que en el Plan de Tratamiento de los Riesgos del Proceso de Sistemas y Seguridad de la Información no se determinaron los indicadores de eficacia y de efectividad, como lo señala la Guía.
En consecuencia, la medición de la gestión del Plan de Tratamiento es parcial porque no se determina la eficacia y efectividad de dichos planes, sólo se calcula el número de veces que se realiza la actividad propuesta.
Hecho que incumple el numeral 3.3 Monitoreo y revisión subtema "Indicadores - gestión del riesgo de seguridad digital" de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 4 de octubre de 2018.

En la respuesta el Proceso afirma que *"…no se acepta la no conformidad ya que el proceso ha atendido lo indicado por la Oficina de Planeación al respecto y en los formatos provistos para este propósito*"
No obstante, la responsabilidad de establecer los riesgos del Proceso y su tratamiento es del líder y de su equipo de trabajo, la OAP apoya y asesora sobre la aplicación de la metodología, pero debe existir al interior del equipo personas que se apropien de los conceptos y técnicas para gestionar los riesgos de seguridad de la información con el fin de cumplir con los lineamientos establecidos por la Corporación y el DAFP. Por lo tanto, se ratifica la No Conformidad y se debe formular el respectivo plan de mejoramiento.

2.15 Se evidenció que la herramienta utilizada para la liquidación de las primas técnicas presenta errores en su funcionalidad y en el seguimiento realizado por el Proceso de Sistemas y Seguridad de la Información al caso radicado en la mesa de ayuda, se determinó que el archivo se encuentra protegido por contraseñas y no es posible modificarlo. Además, se requiere un programador que conozca de Visual Basic.
En consecuencia, se presenta riesgo de errores en las liquidaciones de las primas técnicas.

Hecho que incumple el numeral 6.2.1 Resolver y documentar el Incidente o Requerimiento de Segundo Nivel del Procedimiento Atención de Soporte Tecnológico SSI-PR003 y los literales a. "Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que lo afecten" y e. "Asegurar la oportunidad y confiabilidad de la información y de sus registros" del artículo 2º Objetivos del sistema de Control Interno de la ley 87 de 1993.

3 OPORTUNIDADES DE MEJORA

3.1 Se observó que en el diligenciamiento de la Matriz de Riesgos cuando el tratamiento del riesgo residual se ubica en zona baja es "Aceptar" como quedo plasmado en la "*Guía de Política de Administración de Riesgo*" GMC-GU-002 del 18 de noviembre de 2019, Sin embargo, no aparece este concepto sino el de "Asumir", por tanto, se recomienda modificar la Matriz de Riesgos, para que sea coherente con lo reflejado en la Guía.

3.2 Es necesaria la actualización de los procedimientos del Proceso de Sistemas y Seguridad de la Información, así como, del Manual de Políticas de Seguridad de la Información, para que sirvan de guía en la ejecución de las actividades del Proceso y de la Corporación.

3.3 La entidad debe disponer de los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad digital, tales como:
Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.
Recursos económicos para la implementación de controles de mitigación de riesgos.
Recursos para los aspectos de mejora continua, monitoreo y auditorias.

3.4 Trabajar en el Equipo Técnico de Seguridad de la Información (Resolución 388 de 2019) las alternativas para la implementación de las Políticas de Gestión Gobierno Digital y Seguridad Digital con base en el diagnóstico realizado en el 2019.

1. VERIFICACIÓN DE PLANES DE MEJORAMIENTO DERIVADOS DE AUDITORÍAS ANTERIORES

NO CONFORMIDADES 2018

10.2.8 Se evidenció que no se ha realizado ninguna actividad relacionada con IMPLEMENTACION DE LA LEY 1581 /2012 PROTECION DE DATOS PERSONALES que tiene objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

ACCION PROPUESTA.

Acción Correctiva:

- El proceso de Sistemas y Seguridad, radicó solicitud de contratación para los servicios de consultoría para la implementación de un programa integral de gestión de protección de datos personales en el marco de la ley 1581 de 2012 y la cual fue radicada el 18 de abril con Cordis No. 2018IE4965 y en el Fondo Cuenta en abril 6 de 2018 con CORDIS No. 2018IE62736.

Acción Preventiva:

- Realizar seguimiento a la contratación

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.

- El Proceso reportó que para efectuar los trámites respectivos nuevamente radicó el 14 de febrero de 2019 a la Directora Administrativa (e), la Ficha Técnica para la contratación de una consultoría para la Implementación de un Programa Integral de Gestión de Protección de Datos Personales, solicitud que ya se había realizado en abril de 2018.

- El 8 de julio de 2020 el Proceso SSI informó: "*Se considera que se han realizado las acciones necesarias para la implementación de la política de protección de datos personales, si bien por motivos ajenos al proceso no se realizó la contratación solicitada, si se adelantaron actividades que llevaron a la actualización y aprobación del manual de política de protección de datos…*

"*SSI-MA-002 Manual de política de protección de datos V02.pdf" con actualización del 3 de junio de 2020…* "
CONCLUSIÓN: - De acuerdo con el seguimiento reportado y que el Proceso adelantó actividades para la actualización y aprobación del Manual de Política de Protección de Datos versión 2, se califica la acción como cerrada. - En razón a que el Proceso no es responsable de la suscripción de los contratos, se califica la acción como cerrada.

10.2.9. Se evidencia que el aplicativo liquidación de primas técnicas código TH-PR006-FO25 continua teniendo falencias que no permiten la ejecución eficiente de la asignación de prima técnica este proceso es llevado a cabo en cuadro de Excel sin la seguridad y confiabilidad que requiere este importante procedimiento, por otra parte es importante mencionar que este tema fue una hallazgo evidenciado por la contraloría que indica lo siguiente "2.1.1.1 observación administrativa por falta de controles efectivos en la evaluación, revisión y aprobación en el proceso de primas técnicas a los funcionarios del concejo de Bogotá". Si bien este aplicativo ya había sido revisado con anterioridad por la oficina de sistemas, este aplicativo continúa presentado errores lo que conlleva a que la liquidación se realice de manera manual y revisada de 3 a 4 veces para evitar posibles equivocaciones, en el entendido que la acción de control no fue efectiva, este hallazgo continua en auditoría interna hasta que la oficina de sistemas ajuste el aplicativo y le permita al procedimiento de primas técnicas desarrollar su gestión interna más eficientemente y evitar la materialización de los riesgos.
ACCION PROPUESTA. Acción Correctiva: Con el acompañamiento del Proceso de Sistemas se revisará cada dos meses el funcionamiento correcto del aplicativo de Excel y se dejará constancia de ello en acta.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO Con el apoyo de la Oficina de Sistemas ya fue corregido el error presentado en la herramienta de Excel. El Proceso de SSI reportó que el 14/01/2020 se reunió con la funcionaria encargada de primas técnicas, donde ella expuso la necesidad de revisar el formato en Excel TH-PR006-F025. Por lo tanto, se comprometió a crear el caso en la mesa de servicios (Se identifica con el caso 32067). Luego el 11 de marzo de 2020 se realizó reunión del Proceso de Sistemas con la funcionaria de primas técnicas de la cual se concluyó que el archivo se encuentra protegido por contraseñas y no es posible modificarlo. Además, se requiere un programador que conozca Visual Basic y actualmente el Concejo de Bogotá D.C., no cuenta con una persona con estos conocimientos.
CONCLUSIÓN Se verificaron las actas de acompañamiento del Proceso de Sistemas y Seguridad de la Información para verificar el funcionamiento de la herramienta en Excel para liquidar las primas técnicas (formato TH-PR006-F025). El tiempo de ejecución venció el 12 de diciembre de 2019, sin embargo, se cierra la acción en forma extemporánea.

NO CONFORMIDADES 2019

10.2.1 En relación con la Planeación del Sistema de Seguridad de la información se estableció que el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC, no ha sido aprobado por el Comité de Seguridad de la Información y por ende, no se encuentra publicado en el link de planes institucionales 2019 de Transparencia y acceso a la información. Para la vigencia 2019, los planes de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, de Seguridad y Privacidad de la Información y el de Continuidad del Negocio no fueron aprobados por el Comité de Seguridad de la Información; situación que vulnera lo definido en los numerales 3, 6, 9 y 10 del Artículo 3 "Funciones del Comité de Seguridad de la Información" de la Resolución 934 de 2016 "Por la cual se reglamenta el Comité de Seguridad de la Información en el Concejo de Bogotá D.C. y se deroga la Resolución No.577 del 2014"

ACCION PROPUESTA.
Corrección:
- Realizar aprobación por parte del Comité Institucional de Gestión y Desempeño del PETIC, el cual mediante resolución 388 de 2019 recogió el Comité Técnico de seguridad de la información.
Correctivas:
- Llevar el Plan de Tratamiento de Riesgos de Seguridad de la Información y el Plan del Modelo de Seguridad y Privacidad de la Información a aprobación del Comité Institucional de Gestión y Desempeño.
- Revisar y aprobar el Plan de Continuidad de Negocio de acuerdo al procedimiento de control de documentos del SIG.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.-
- Se corroboró que en el Acta 001 del 29 de mayo de 2019 del Comité Institucional de Gestión y Desempeño se aprobó el PETIC de la Corporación.
- En el Acta 002 de julio 22 de 2019 del Comité Institucional de Gestión y Desempeño se aprobó la modificación de los planes de Gobierno Digital: Plan de Tratamiento de Riesgos de Seguridad de la Información y el Plan de Modelo de Privacidad y Seguridad de la Información.

- El Proceso de SSI reportó que "*Quedo pendiente la presentación y aprobación del plan de continuidad de negocio el cual debe presentarse en el próximo Comité Institucional de Gestión y Desempeño* "

El 8 de julio de 2020 se informó "…*El proceso en cumplimiento con lo acordado procedió a la elaboración y presentación del procedimiento de continuidad de negocio del subsistema de seguridad de la información, el cual fue aprobado en la reunión del comité SIG del 24 de enero de 2019 como se puede evidenciar en el acta de dicho comité…*".
Sin embargo, este soporte no es válido porque en el Comité del SIG 001 realizado el 14 de enero de 2019, se aprobó entre otros documentos el Procedimiento Continuidad del Negocio SGSI.

CONCLUSIÓN.-
- El Proceso de Sistemas cumplió con la ejecución de las acciones relacionadas con la aprobación por parte del Comité Institucional de Gestión y Desempeño (CIGD) del PETIC, el Plan de

Tratamiento de Riesgos de Seguridad de la Información y el Plan del Modelo de Privacidad y Seguridad de la Información; en consecuencia, estas dos (2) acciones se califican como cerradas.

- No se ha realizado la revisión y aprobación del Plan de Continuidad de Negocio del Concejo de Bogotá, D.C. en el Comité Institucional de Gestión y Desempeño, pese a que dicha acción culminó el 30/10/2019, por lo tanto, esta acción se califica como abierta.

10.2.2 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.

Lo anterior incumple el control A.8.1.1 Inventario de Activos "Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se deben elaborar y mantener un inventario de estos Activos" de la Norma ISO 27001:2013. Además de los artículos 37 y 38 del Decreto 103 de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

También se transgrede el numeral 6.2 Valoración de los activos de información donde se establece que los activos de información se deben valorar en términos de confidencialidad, integridad y disponibilidad y la suma de estos conceptos corresponde al valor del activo el cual "... permite determinar que activos (valor crítico y alto) se tendrán en cuenta para la identificación y valoración de riesgos de seguridad de la información" del documento SSI-Gu005 "Guía para la identificación y valoración de Activos" Versión 1 del 27 de Octubre de 2017.

ACCION PROPUESTA. -
Corrección.
- Actualizar la información del inventario de activos de información

Correctiva:
- Socializar a los líderes de proceso y gestores de mejora institucional el formato de inventario de activos y realizar acompañamiento para su diligenciamiento.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO. -

- El Proceso reportó "*… se identificó que existen falencias en las herramientas documentales para realizar la actualización de los activos de información, donde se deben presentar en Comité los nuevos procedimientos, guias y formatos ajustados para realizar esta actividad*". El 8 de julio de 2020 el Proceso informó: "*La actualización del inventario de activos de información corresponde a cada líder de proceso, con el fin de brindar las herramientas necesaria el proceso de sistemas y seguridad de la información realizó las socializaciones del formato con los procesos y gestores de mejora…*" - Se verificó que el Proceso SSI adelantó reuniones (realizadas entre agosto y octubre de 2019) con los demás procesos para socializar la Metodología para determinar los tipos de activos de información y el formato PR008-F01 "Planilla de Inventarios de Activos de Información".
CONCLUSIÓN. – - Se evidenció que en julio de 2020 el inventario de activos de información no está actualizado, pese a que la acción culminó el 30 de septiembre de 2019. Por lo tanto, se califica como abierta. - Se corroboró que se realizó la socialización a los procesos y gestores de mejora institucional de la Metodología y formato PR008-F01. Por lo tanto, esta acción se califica como cerrada.

10.2.3 El Sistema de Seguridad de la Información cuenta con un Mapa de Riesgos, el cual fue elaborado en el año 2017, por la Empresa Password Consulting Services SAS, que incluía inicialmente 58 riesgos y en enero de 2019 fue modificado, agregándole dos (2) para un total de 60 riesgos. Se definieron riesgos para los procesos de evaluación independiente, talento humano, gestión financiera, recursos físicos, sistemas y seguridad de la información y todos los procesos. A este mapa se le definió un seguimiento semestral; sin embargo, no se evidenció una apropiación del tema sobre la gestión de riesgos por parte del Proceso de Sistemas y Seguridad de la Información, tampoco se documentaron seguimientos. Frente a la modificación del Mapa de Riesgos en el año 2019, no se tuvo en cuenta la guía establecida por el DAFP para la administración del riesgo y el diseño de controles en entidades públicas (octubre de 2018) ni el inventario de los activos de información se encuentra incompleto y desactualizado.
ACCION PROPUESTA. Corrección: - Realizar la revisión y ajuste de los Mapas de Riesgos de Seguridad de la información conforme a lo establecido al procedimiento de Administración de riesgos. Correctiva: - Realizar el seguimiento, verificación y ajuste de los riesgos de seguridad de la información conforme a la metodología aprobada en la Entidad.
SEGUIMIENTO OFICINA CONTROL INTERNO. - La Dirección Administrativa cuenta con los Mapas de Riesgos aprobados por los líderes de procesos y se cuenta con acceso de consulta en la red de la Corporación U:\Administración de Riesgos\2019 de acuerdo con los lineamientos del DAFP.

- En el 2019 no se realizó la revisión de la aplicación de los controles ni la gestión del riesgo por parte de los líderes de los procesos, así como, tampoco su monitoreo por parte de la Oficina Asesora de Planeación, pese a que fueron aprobados por los líderes de los procesos.

El 8 de julio de 2020 el Proceso reportó "*Dada la observación realizada por la auditoria relacionada con la inclusión de los activos de información se realizará una nueva definición del mapa de riesgos de seguridad de la información*"

CONCLUSIÓN.-
- Con la actualización de los activos de información se revisará y ajustará el seguimiento al mapa de riesgos de seguridad de la información. Por tal motivo, la acción se califica como abierta.

- Se realizará el seguimiento y verificación al mapa de riesgos de seguridad de la información. Por tal motivo, la acción se califica como abierta.

10.2.4. Se observó que el Sistema de Gestión de Seguridad de la Información presenta debilidades en el monitoreo y seguimiento de las actividades propuestas (proceso, riesgos, planes de mejoramiento, etc.). Lo anterior incumple lo señalado en la Norma ISO 27001:2013, numeral 9.1 Seguimiento, medición, análisis y evaluación literales a. "A qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información", b. "los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable para asegurar resultados válidos" c. "Cuando se deben llevar a cabo el seguimiento y la medición", d. "Quien debe llevar a cabo el seguimiento y la medición", e. "Cuando se deben analizar y evaluar los resultados del seguimiento y de la medición", y f. "Quien debe analizar y evaluar estos resultados" "la organización debe conservar información documentada apropiada como evidencia de los resultados de monitoreo y de la medición".

ACCION PROPUESTA.-
Correctivas:
- Establecer los indicadores del SGSI en la Ficha aprobada en el SIG, realizando seguimiento de los mismos conforme a su frecuencia.
- Establecer cuadro de seguimiento para generar las alertas necesarias para el monitoreo y seguimiento a las diferentes actividades del Sistema de Gestión de Seguridad de la Información

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.-
- El proceso informó que cuenta con tres (3) indicadores de gestión que serán aplicados semestralmente.

- El 8 de julio de 2020 el Proceso informó "*Para la definición de los indicadores se utilizó el formato suministrado por la Oficina Asesora de Planeación, en el cual al final del cuadro se encuentran las casillas para el respectivo seguimiento trimestral…"*

De lo anterior, se ratifica que no se evidenció la elaboración del cuadro de seguimiento para el monitoreo y seguimiento a las diferentes actividades del Sistema de Gestión de Seguridad de la Información.

CONCLUSIÓN.-
- En razón, a que los indicadores fueron aprobados y su medición se realizará a partir de junio de 2020, se decide cerrar la acción.
- Respecto al cuadro de seguimiento para el monitoreo a las diferentes actividades del Sistema de Gestión de Seguridad de la Información, no se soportó su elaboración, porque sólo anexan el cuadro de seguimiento al plan de mejoramiento o el plan de acción.

Adicionalmente, el tiempo de ejecución para la acción venció el 30 de julio de 2019. Por lo tanto, se califica como abierta.

10.2.5 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.

ACCION PROPUESTA.-
Correctiva:
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.-
El Proceso de SSI anexó en julio 8 de 2020 el borrador del nuevo procedimiento para realizar las actividades de identificación, clasificación, valoración, etiquetado y manejo de activos de información,

CONCLUSIÓN.-
El tiempo de ejecución de la acción venció el 30 de octubre de 2019, por tal razón, se califica como abierta.

10.2.6 Efectuado el seguimiento al cumplimiento de las acciones concertadas en los planes de mejoramiento suscritos por el Proceso de Sistemas y Seguridad de la Información con la empresa certificadora SGS Colombia y con la Oficina de Control Interno, se determinaron los siguientes resultados:

Tabla No. 1
Seguimiento Planes de Mejoramiento SGSI

AUDITORÍA CANTIDAD DE NO CONFORMIDADES CANTIDAD DE ACCIONES
DEFINIDAS AVANCE PROMEDIO
Externa de Certificación SGS –

No Conformidades Mayores 8 34 37.7%
Externa de Certificación SGS – No Conformidades Menores 7 34 18.2%
Interna de OCI 3 7 30.0%
TOTALES 18 75
Fuente: Información Entregada al Equipo Auditor

El Plan de Mejoramiento se revisó con corte al 30 de marzo de 2019 y consta de un total de 75 acciones distribuidas entre correctivas, preventivas y de corrección.
Las 34 acciones definidas para las No Conformidades Mayores estaban programadas para culminar el 30 de abril de 2019, de las cuales se cumplieron cuatro (4) al 100% y 13 presentaron una calificación entre el 50% y el 80%.

Respecto a las 34 acciones determinadas para las No Conformidades Menores, se cumplió una (1) con el 100% y cinco (5) se evaluaron en el rango entre el 50% y el 80%.
Es de resaltar para este grupo que 21 acciones que representan los 62% del total definidas, finalizaban ejecución en abril de 2019, pero no se evidenció avance para 14 de ellas.

Finalmente, para las acciones derivadas de la Auditoría Interna se estableció que una (1)
Logró el 100% y cuatro (4) se calificaron en un rango del 20% al 50% de avance. Sin embargo, las acciones se encuentran en ejecución hasta diciembre de 2019 y por tal razón, no se efectúa su cierre total.
Para conocer el seguimiento puntual se anexan los papeles de trabajo correspondientes a los planes analizados.
Por lo anteriormente presentado, se determinó que el proceso de Sistemas y Seguridad de la Información no dispone de un mecanismo de seguimiento y control al cumplimiento de las acciones concertadas en los diferentes planes de mejoramiento suscritos, con la disposición de los respectivos soportes. Lo que incumple el Numeral 10.1 No Conformidades y Acciones Correctivas" literales c. "Implementar cualquier acción necesaria" d. "Revisar la eficacia de las acciones correctivas tomadas" e. "Hacer cambios al sistema de gestión de la seguridad de la Información, si es necesario". Además, "La organización debe conservar información documentada adecuada, como evidencia de: f. La naturaleza de las no conformidades y cualquier acción posterior tomada y g. Los resultados de cualquier acción correctiva" de la Norma ISO 27001:2013.

ACCION PROPUESTA.-
Correctiva:
- Establecer cuadro de seguimiento para generar las alertas necesarias para el monitoreo y seguimiento a las diferentes actividades del Sistema de Gestión de Seguridad de la Información. El cuadro de seguimiento establece los responsables y la periodicidad para evidenciar el cumplimiento de las actividades.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.-
El Proceso presentó como soporte de esta acción las matrices para el seguimiento a los planes de mejoramiento de las Auditorías Internas 2018 y 2019, así como, los derivados de las auditorías de certificación realizadas por SGS.

CONCLUSIÓN.-

Pese a la elaboración de las matrices para el seguimiento a los Planes de Mejoramiento del Proceso SSI, se observó que en los cuadros allegados no se definió el periodo de inicio y finalización de cada una de las acciones que es un aspecto clave para determinar su cumplimiento oportuno. En consecuencia, el tiempo para la ejecución de esta acción venció el 17 de junio de 2019 y se califica como abierta.

10.2.8 No se evidenciaron en los informes de gestión de servicio de mesa de ayuda generados por el contratista, los reportes de control de inventarios de hardware y software el cual según el numeral 8.1 del anexo FICHA TÉCNICA del contrato No 180353-0-2018, celebrado con la Unión temporal SDH-TSSYRTECT-2018. El reporte solicitado se encuentra alineado también con los controles A.15.1.3., "cadena de suministro de tecnología de información y comunicación" y A.8.1.1. "Inventario de activos" de la norma ISO 27001:2013, ya que, para éste último, si bien existe en el Concejo de Bogotá una planilla de inventario de activos de información código: SSI-PR0008-F01, es importante mantener este inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo/personal, nuevos sistemas y cambios de Tecnologías de Información.
ACCION PROPUESTA.- Correctiva: Realizar el levantamiento del inventario de hardware y software por parte del contratista de Mesa de Ayuda y mantener la obligación de mantener actualizado este inventario en el contrato.
SEGUIMIENTO OFICINA CONTROL INTERNO.- El proceso reportó el 8 de julio de 2020 lo siguiente: "*A la fecha se cuenta con el inventario actualizado, en el mes de marzo, se realizó un seguimiento el cual se encuentra documentado en Excel, con el contratista se programaron actividades para subirlos a la herramienta ARANDA pero debido a la contingencia por la pandemia de COVID 19 se suspendieron las actividades, se tiene como evidencia el documento en Excel con la información actualizada…*"
CONCLUSION: Pese a que el Proceso reportó que cuenta con el inventario actualizado en el mes de marzo y lo adjunto a esta Oficina; se determinó que sólo hace referencia al hardware (equipos de escritorio y portátiles) de la Corporación y no se relaciona el inventario vigente de software. En consecuencia, la ejecución de esta acción venció el 30 de enero de 2020 y por ende, se califica como abierta.

10.2.9. Se determinó que no se elaboró el Informe de Capacidad Trimestral correspondiente al primer trimestre del año 2019, lo que incumple el control A.12.1.3 "Gestión de Capacidad" de la Norma ISO 27001:2013 y los numerales 6.3 "Realizar Análisis de Capacidad Actual" y 6.4 "Revisar el Informe Trimestral de Capacidad", del procedimiento Gestión de la Capacidad SSI-PR006 versión 3 de 2017.
ACCION PROPUESTA.- Corrección: -Hacer el informe de capacidad del primer trimestre de 2019

Correctivas: -Realizar los informes de capacidad conforme a lo establecido en el procedimiento de Gestión de Capacidades. -Revisar los informes de capacidad trimestral para detectar desviaciones.
SEGUIMIENTO OFICINA DE CONTROL INTERNO.- - El informe del primer trimestre de capacidad fue elaborado conforme a los lineamientos establecidos en el procedimiento de Gestión de Capacidades. - También, se elaboraron los Informes Trimestrales (abril – junio y julio - septiembre) del año 2019, sobre la capacidad de los recursos de hardware y software en la infraestructura tecnológica de la Corporación. - El 8 de julio de 2020 el Proceso reportó: "*Se tiene el documento de análisis de la capacidad realizado al interior del proceso recientemente.* *Este documento se ha empleado para el determinar los nuevos requerimientos por parte del proceso en temas de infraestructura…"* No se soportaron las medidas adoptadas con base en las recomendaciones derivadas de los informes de capacidad.
CONCLUSIÓN.- - El Proceso presentó el Informe del Primer Trimestre, por tanto, esta acción se califica como cerrada. - Se corroboró que se elaboraron los Informes Trimestrales (abril – junio y julio - septiembre) del año 2019, sobre la capacidad de los recursos de hardware y software en la infraestructura tecnológica de la Corporación, por tanto, esta acción se califica como cerrada. - Pese a que el Proceso elaboró un esquema de revisión de desviaciones (no posee fecha), no se documentó que el Informe de Capacidad sirvió para el determinar los nuevos requerimientos en temas de infraestructura. En consecuencia, esta acción se califica como abierta porque culminó su tiempo de ejecución el 23 de Mayo de 2020.

10.2.10 Se observó que el Proceso de Sistemas y Seguridad de la Información posee unos cuadros en Excel donde detalla el hardware y software de la Corporación, sin embargo, estos archivos se encuentran desactualizados desde aproximadamente octubre del año 2018, porque aparecen como responsables de los equipos personas que se desvincularon de la entidad o cambiaron de área. Adicionalmente, en los cuadros de software no se identifican responsables de su custodia. Situación que indica que dicho inventario no se mantiene y no cumpliría su función como una herramienta de control de estos bienes. Lo que representa un riesgo de pérdida o daño de los equipos que podría afectar la operación de la Corporación. Hecho que transgrede el control A.8.1.1 "Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos" de la norma ISO 27001:2013.
ACCION PROPUESTA.-

Correctiva: Realizar el levantamiento del inventario de hardware y software por parte del contratista de Mesa de ayuda y mantener la obligación de mantener actualizado este inventario en el contrato.
SEGUIMIENTO CONTROL INTERNO.- El proceso reporta que "*Se realizo el levantamiento del inventario de hardware y la depuración del inventario de software de la Corporación*" Sin embargo, está pendiente la entrega del inventario actualizado. El 8 de julio de 2020 El Proceso SSI comentó "*A la fecha se cuenta con el inventario actualizado, en el mes de marzo, se realizó un seguimiento el cual se encuentra documentado en Excel, con el contratista se programaron actividades para subirlos a la herramienta ARANDA pero debido a la contingencia por la pandemia de COVID 19 se suspendieron las actividades,* *Este documento se pone a disposición como evidencia,* *Por lo anterior solicitamos el cierre de la no conformidad*".
CONCLUSIÓN. – Pese a que el Proceso reportó que cuenta con el inventario actualizado en el mes de marzo y lo adjunto a esta Oficina; se determinó que sólo hace referencia al hardware (equipos de escritorio y portátiles) de la Corporación y no se relaciona el inventario vigente de software. En consecuencia, el tiempo programado para la ejecución de la acción culminó el 30 de enero de 2020 y por ende, se califica como abierta.

10.2.11. Se determinó que no se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en los sistemas (Directorio Activo) y aplicaciones (PERNO, CORDIS Y EXCHANGE) de la Corporación, situación que transgrede el control A.9.2.5 "Revisión de los derechos de acceso de usuarios. Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares" de la Norma ISO 27001:2013.
ACCION PROPUESTA.- Correctiva: Revisar con el proceso de Talento Humano las responsabilidades definidas en el procedimiento de acceso lógico para desarrollar de forma adecuada la revisión de derecho de acceso
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.- Se evidenciaron correos electrónicos enviados por la Dirección Administrativa – Talento Humano, donde le informa al Proceso de Sistemas y Seguridad de la Información el listado de posesionados, con fecha de ingreso, cargo, área, entre otra información; con el propósito de actualizar las bases de datos de las personas que tienen derecho de acceso a la red de la Corporación
CONCLUSIÓN.- Se evidenció la ejecución de la acción propuesta y pese a que la acción culminó el 30 de noviembre de 2019, se califica como cerrada. .

10.2.12. Se observó durante la ejecución de auditoría en la Intranet del Concejo, la publicación del Plan de Continuidad de Negocio (PCN) Versión 2, que fue elaborado por la empresa Password en noviembre de 2017. A este Plan no se le realizaron pruebas, como se definió en dicho documento: "…El plan de continuidad de negocio en el Concejo de Bogotá, D.C. debe ser probado al menos una vez al año". "Es responsabilidad de los líderes de procesos gestionar la realización de una prueba anual en la que se verifique la operación de los procesos y componentes de contingencia…". Es decir, el Plan de Continuidad del Negocio esta desactualizado no se evalúo y no se le practicaron pruebas de continuidad del negocio. Esta situación transgrede lo definido en el Control A.17.1.1 "Planificación de la continuidad de la seguridad de la información", A.17.1.2 "Implementación de la continuidad de la seguridad de la información" y A.17.1.3 "Verificación, revisión y evaluación de la continuidad de la seguridad de la información" de la Norma ISO 27001:2013.
ACCION PROPUESTA.- Correctiva: Realizar las pruebas de continuidad de negocio y documentar las mismas.
SEGUIMIENTO OFICINA CONTROL INTERNO.- El Proceso de Sistemas y Seguridad de la Información reportó que: "*Se realizó en el mes de noviembre la planificación de una prueba de continuidad de negocio, para garantizar la continuidad del servicio de seguridad perimetral del Concejo de Bogotá, la cual no fue posible realizarla, debido a que no contaba con el servicio de monitoreo de la plataforma de seguridad perimetral por parte del proveedor del servicio y que de efectuar la prueba se debía realizar una ventana de mantenimiento y no era viable, porque la infraestructura de TI debía estar en alta disponibilidad debido a los cambios del nuevo periodo legislativo del Concejo de Bogotá D.C*" En julio 8 de 2020 el Proceso comunicó: "*Se cuenta con el documento preliminar para la realización de las pruebas de continuidad de negocio del subsistema de seguridad de la información, debido a la contingencia por el Covid 19 no fue posible llevarlas a cabo en el plazo programado.* *Se puede evidenciar que los sistemas de contingencia se encuentran operativo y funcionales ya que a pesar de la imposibilidad de asistir a la corporación el proceso a mantenido la accesibilidad a los diferentes sistemas de forma no presencial*".
CONCLUSIÓN. – Si bien es cierto la Corporación en la época de pandemia ha funcionado, las pruebas del Plan de Contingencia poseen unas especificidades técnicas que es necesario desplegar (como se reporta en la primera respuesta) y documentar, las cuales no se han desarrollado en el tiempo programado de ejecución que venció el 27 de mayo de 2020. En consecuencia, la acción se califica como abierta.

10.2.13. Se verificó que el navegador que soporta la página web del Concejo de Bogotá D.C. no se encuentra certificado, no posee cifrado y no es seguro, por ello cuando se ingresa a dicha página aparece un mensaje donde se enuncia que "La conexión con este sitio web no es segura" porque no dispone del protocolo HTTPS. Lo que transgrede el control A.14.2.7 "Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo

de sistemas contratados externamente", de la Norma ISO 27001:2013. Además, incumple el literal a) "Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten" y 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" del artículo 2º de la ley 87 de 1993.
ACCION PROPUESTA.- Correctiva: Realizar las gestiones necesarias para obtener el certificado de sitio seguro de la Página Web y la Intranet del Concejo de Bogotá, D.C.
SEGUIMIENTO OFICINA CONTROL INTERNO. - El Proceso reportó que el 2 de agosto de 2019, solicitó a la SDH la creación de línea para la renovación de los certificados seguros SSL de la Corporación. Además, en el desarrollo de la auditoría anexó la Ficha Técnica y la Solicitud de Contratación con el objeto de "*Proveer certificados de servidor seguro SSL para el Concejo de Bogotá*", documentos que fueron radicados en el 2020 por Daniel García Cañón Director Administrativo ante la SDH para iniciar el proceso de contratación.
CONCLUSIÓN. - Se verificó que el Proceso desarrollo la acción propuesta para realizar la contratación. Pese a que el tiempo para la ejecución venció el 30 de diciembre de 2019, se califica la acción como cerrada.

10.2.14. 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. Situación que transgrede lo definido en el numeral 10.2 Mejora Continua "La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información" de la Norma ISO 27001:2013.
ACCION PROPUESTA.- Correctivas: - Revisar en mesa de trabajo los planes de mejora actuales a cargo del proceso de Sistemas y Seguridad de la Información y solicitar los ajustes en caso de ser necesario mediante correo o memorando. - Realizar el seguimiento a los planes de mejoramiento del proceso y del SGSI.
SEGUIMIENTO OFICINA CONTROL INTERNO. - El Proceso no presentó evidencia de la revisión en mesa de trabajo de los planes de mejora a su cargo. Sin embargo, efectuó solicitud de ampliación de tiempo para siete (7) No Conformidades,

por medio del memorando con radicado 2019IE18539 del 31 de diciembre de 2019 y con el radicado No. 2020IE2326 del 31 de enero de 2020, se realizó una nueva solicitud de prórroga de ejecución para siete (7) No Conformidades. - El Proceso anexó matrices por medio de las cuales se relacionó el seguimiento al Plan de Mejoramiento de las Auditorías Internas 2018 y 2019, así como, los derivados de las auditorías de certificación realizada por SGS.
CONCLUSIÓN.- - Una vez verificado lo realizado por el Proceso se considera que la acción se califica como cerrada. - Pese a la elaboración de las matrices para el seguimiento a los Planes de Mejoramiento del Proceso SSI, se observó que en los cuadros allegados no se definió el periodo de inicio y finalización de cada una de las acciones que es un aspecto clave para determinar su cumplimiento oportuno. En consecuencia, el tiempo para la ejecución de esta acción venció el 17 de junio de 2019 y se califica como abierta.

10.2.15. Se observaron debilidades en la definición de la necesidad del Contrato 180436-0-2018 cuyo objeto es la Prestación de Servicios de recuperación de Información de cintas históricas del Concejo de Bogotá, porque en primera instancia solo se exigió la certificación en ISO 27001:2013, posteriormente le agregaron la exigencia en la Norma ISO 9000, pero sin especificar la versión y finalmente en la etapa de las observaciones, con la Adenda 2, se eliminó este requisito, lo que genera incertidumbre y confusión sobre la certeza técnica de exigir desde la necesidad y anexo técnico la certificación de norma ISO y su versión vigente a los oferentes. Hecho que transgrede el principio de planeación artículo 25 de la Ley 80 de 1993, numerales 7 “La conveniencia o inconveniencia del objeto a contratar y las autorizaciones y aprobaciones para ello, se analizarán o impartirán con antelación al inicio del proceso de selección del contratista o al de la firma del contrato, según el caso” y 12 “Previo a la apertura de un proceso de selección, o a la firma del contrato en el caso en que la modalidad de selección sea contratación directa, deberán elaborarse los estudios, diseños y proyectos requeridos, y los pliegos de condiciones, según corresponda…”.
ACCION PROPUESTA.- Correctiva: Establecer punto de control de revisión de los requisitos solicitados en la contratación por parte del Sistemas y Seguridad de la Información.
SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.- El Proceso reportó en julio 8 de 2020 que: “*… realiza reuniones al interior en las que se socializan las fichas técnicas y los requisitos para los diferentes procesos de contratación, también se atienden las observaciones realizadas por la Dirección de Informática y Tecnología de la Secretaría Distrital de Hacienda como entidad compradora*”
CONCLUSIÓN.-

Pese a que el Proceso de SSI realiza reuniones con el equipo de trabajo y con *la* Dirección de Informática y Tecnología de la Secretaría Distrital de Hacienda para estudiar los procesos de contratación que desarrollan, no se aportan actas u otros documentos que las sustenten. El tiempo de ejecución de la acción venció el 30 de noviembre de 2019. Por lo anteriormente expuesto, se califica como abierta.

10.2.16. El Proceso de Sistemas y Seguridad de la Información definió la acción correctiva "…4. Establecer un Acuerdo Interadministrativo entre el Concejo de Bogotá y la Secretaría Distrital de Hacienda para los temas del Datacenter" y en cumplimiento de dicha acción aportó el 29 de abril del presente año, un Convenio Interadministrativo celebrado con la Secretaría Distrital de Hacienda, con el siguiente comentario "Folios 14 al 16 - Convenio inicial que se realizó con la Secretaría de Hacienda, firmado por el subdirector de infraestructura de SHD, el asesor de la DIT de la SHD, y por el Concejo de Bogotá la Doctora Efvanni Paola Palmarini Directora Financiera y administrativa (E) y el responsable del Proceso de Sistemas; para tal efecto este documento debe ser ampliado, realizar un nuevo acercamiento y firmarlo por las partes" Al revisar dicho documento se observó que le faltan formalidades para ser un Convenio Interadministrativo como el acto administrativo donde se justifique contratar bajo la modalidad de contratación directa, la minuta carece de un número consecutivo que lo identifique, no posee fecha de suscripción que permita determinar su vigencia, no se identifican jurídicamente las entidades intervinientes por su naturaleza y objeto.
ACCION PROPUESTA.- Correctiva: Presentar la necesidad de gestionar el convenio interadministrativo con la SHD con los temas de Seguridad de la Información.
SEGUIMIENTO OFICINA CONTROL INTERNO.- Se verificó comunicación con fecha del 31 de Mayo de 2019 radicado número 2019EE3626 dirigido al Dr. Gerson Granados Villamil Director de Informática y Tecnología Secretaría Distrital de Hacienda con el fin de "*Aunar esfuerzos para la realización conjunta de actividades contractuales…*" el documento cuenta con formato de Solicitud de Contratación GF-PR006-F01 donde se evidencia la necesidad de crear un convenio con los temas de Seguridad de la Información. Adicionalmente, el Proceso reportó "*En el primer semestre del año 2019 se gestionó un convenio interadministrativo entre el Concejo de Bogotá D.C. y la SDH*" y de acuerdo con el seguimiento realizado con el responsable del SSI, la suscripción del Convenio está a cargo de la SDH y en el área solo se elabora la ficha técnica y la solicitud de contratación. El 8 de julio de 2020 el Proceso comunicó "*Teniendo en cuenta que el informe final del proceso de auditoría interna fue del 9 de mayo de 2019 y el plan de mejora se presentó el 13 de mayo del mismo año, el proceso de sistemas y seguridad de la información de forma proactiva antes de que se aprobara el plan de mejoramiento realizó la acción propuesta con el fin de atender la no conformidad…el proceso cumplió con lo propuesto, pero la decisión de establecer un convenio interadministrativo se encuentra fuera del alcance del proceso*."

CONCLUSIÓN.-
El tiempo para la ejecución de la acción culminó el 30 de diciembre de 2019 y se decide su cierre en forma extemporánea.

2. SEGUIMIENTO MATRIZ DE RIESGOS Y ANÁLISIS DE CONTROLES

RIESGO 1

Perdida, Alteración o indisponibilidad de los servicios de TI y la información por acceso no autorizado a sistemas y servicios, o abuso de derechos de acceso a sistemas y servicios

CLASIFICACIÓN DEL RIESGO
Seguridad de la Información

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
- Revisar y actualizar la política y el manual de políticas de seguridad de la información
- Realizar revisión de la Seguridad de la Información semestralmente por parte de los directivos y jefes de dependencia de la Corporación

SOPORTE:
N.A.

TIEMPO
N.A
INDICADOR:
N.A.

OBSERVACIONES:

- En la gestión de los riesgos de Seguridad Digital no se evidenció el establecimiento del contexto externo e interno ni se actualizó el inventario de Activos de la Información.

- No se definieron en forma individual los riesgos pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

- No se observó la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

- Evaluación del Diseño de los Controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  Se definieron dos controles que cada uno alcanzó una calificación de 100, para un promedio de 100.

  El control 1 mitiga la causa raíz 1, hace referencia al numeral 8.6.2, versión 3 de 2018 del Manual de Políticas de Seguridad de la Información.

  El control 2 mitiga parcialmente la causa raíz 2 y se reseña el Procedimiento de Gestión de Cambios versión 3 de diciembre de 2018, el cual no fue actualizado en el 2019 con el fin de definir controles que cumplieran con los criterios que establece la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.
- Con relación el Plan de Tratamiento de Riesgos no presenta soporte, tiempo ni indicador porque el riesgo residual se ubicó en Zona de Riesgo Bajo y según la "Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019" el tratamiento es Aceptar (es decir, que no se adopta ninguna medida) pero de acuerdo con la guia se realiza seguimiento. No obstante, el Proceso decidió establecer dos actividades de control.

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 2

Pérdida, Alteración o indisponibilidad de los servicios de TI y la información por acceso no interrupción de energía, fallos de hw y daño a equipos del datacenter

CLASIFICACIÓN DEL RIESGO
Seguridad de la Información

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
- Revisar la seguridad de los sistemas de información
- Hacer Seguimiento a la seguridad del datacenter con Secretaria Distrital de Hacienda, estableciendo un convenio interadministrativo para tener un mejor control de los elementos tecnológicos del Datacenter.

SOPORTE:
N.A.

TIEMPO
N.A

INDICADOR:
N.A.

OBSERVACIONES:

- En la gestión de los riesgos de Seguridad Digital no se evidenció el establecimiento del contexto externo e interno ni se actualizó el inventario de Activos de la Información.

- No se definieron en forma individual los riesgos pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

- No se observó la agrupación de activos del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

- Evaluación del Diseño de los Controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  Se definieron siete controles para 6 causas, que alcanzaron una calificación individual de 100, para un promedio de 100. De los cuales se destacan los siguientes:

  El control 1 mitiga parcialmente la causa raíz 1, hace referencia al mantenimiento de los equipos, actividad que es contratada y no se cumple con la elaboración de planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

  El control 3 mitiga parcialmente la causa raíz 3 porque corresponde al Procedimiento del Procedimiento de Continuidad de Negocio del Subsistema de Seguridad de la Información versión 1 de enero de 2019, el cual no fue revisado en la vigencia 2019 con el fin de definir controles que cumplieran con todos los criterios que establece la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.
  Además, en la Corporación no se tiene un Plan de Continuidad de Negocio si no un Plan de Contingencia. Por lo tanto, este control no es fuerte.

- El Plan de Tratamiento de Riesgos no presenta soporte, tiempo ni indicador porque el riesgo residual se calificó en Zona de Riesgo Bajo y según la “Guía de Política de Administración de

Riesgo GMC-GU-002 del 18 de noviembre de 2019" el tratamiento es Aceptar (es decir, que no se adopta ninguna medida) pero de acuerdo con la guia se realiza seguimiento. No obstante, el Proceso decidió estableció una actividad de control.

Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 3

Afectación de la confidencialidad, integridad y disponibilidad de la información debido a las malas prácticas en Seguridad de la Información de los usuarios

CLASIFICACIÓN DEL RIESGO
Seguridad de la Información

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
- Revisar y actualizar de la política y el manual de políticas de seguridad de la información.
- Realizar revisión de la Seguridad de la Información semestralmente por parte de los directivos y jefes de dependencia de la Corporación
- Planear y ejecutar actividades de sensibilización en seguridad de la información

SOPORTE:
N.A.

TIEMPO
N.A

INDICADOR:
N.A.

OBSERVACIONES:

- En la gestión de los riesgos de Seguridad Digital no se evidenció el establecimiento del contexto externo e interno ni se actualizó el inventario de Activos de la Información.

- No se definieron en forma individual los riesgos pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

- No se observó la agrupación de activos del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

- Evaluación del Diseño de los Controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  Se definieron dos controles que cada uno se calificó con 100, para un promedio de 100.

  El control 1 mitiga parcialmente la causa raíz 1 porque hace referencia a la aplicación de las políticas de seguridad de la Corporación, las que abordan diferentes temas de seguridad y el Manual de Políticas se encuentra desactualizado, no se debió calificar el control con 100.

  El control 2 mitiga parcialmente la causa raíz 2 debido a que no es clara la correspondencia del control “Revisión de las Políticas de Seguridad de la Información” con la causa “Falta de capacidad para realizar la aplicación de las directrices y normatividad de la nación…”
  Además, que se contradice con la actividad de control definida “Revisar y actualizar de la política y el manual de políticas de seguridad de la información”.

- Respecto al Plan de Tratamiento de Riesgos no presenta soporte, tiempo ni indicador porque el riesgo residual se calificó en Zona de Riesgo Bajo y según la “Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019” el tratamiento es Aceptar (es decir, que no se adopta ninguna medida) pero de acuerdo con la guia se realiza seguimiento. No obstante, el Proceso decidió establecer tres actividades de control.

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 4

Perdida de confidencialidad, integridad y disponibilidad de los activos de información

CLASIFICACIÓN DEL RIESGO
Seguridad de la Información

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:

- Actualizar el manual de roles y responsabilidades de Seguridad de la Información.
- Actualizar el listado de contactos y grupos de interés de seguridad de la información.
- Coordinar la actualización del listado de activos de información con todos los procesos.

SOPORTE:
N.A.

TIEMPO
N.A

INDICADOR:
N.A.

OBSERVACIONES:

- En la gestión de los riesgos de Seguridad Digital no se evidenció el establecimiento del contexto externo e interno ni se actualizó el inventario de Activos de la Información.

- No se definieron en forma individual los riesgos pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

- No se observó la agrupación de activos del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

- Evaluación del Diseño de los Controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  Se definieron cinco controles para cinco causas, cada control se calificó con 100, para un promedio de 100.

  El control 4 no mitiga la causa raíz 4 porque no existe coherencia entre el control aplicado "*Contacto con los Grupos de Interés Especial*" con la causa "Desactualización del Inventario de Activos de Información" ni tampoco se observa ningún control que mitigue esta causa.

  Se observó de los cinco controles definidos para este riesgo que ninguno mitiga la causa "*No tener claridad en la clasificación y etiquetado de la información*". Por tanto, no debieron tener una calificación de 100.

- El Plan de Tratamiento de Riesgos no presenta soporte, tiempo ni indicador porque el riesgo residual se calificó en Zona de Riesgo Bajo y según la "Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019" el tratamiento es Aceptar (es decir, que no se adopta ninguna medida) pero de acuerdo con la guia se realiza seguimiento. No obstante, el Proceso decidió establecer tres actividades de control.
  Se observó que en el diligenciamiento de la Matriz de Riesgos no se escribió "Aceptar" sino "Asumir".

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 5

Daños en los equipos y la infraestructura del centro de cableado principal

CLASIFICACIÓN DEL RIESGO
Seguridad de la Información

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
Hacer acompañamiento a la implementación del datacenter en la construcción del nuevo edificio del Concejo de Bogotá D.C.

SOPORTE:
Realizar acompañamiento a la implementación de los diseños del nuevo Datacenter y centro de cableado

TIEMPO
Diciembre de 2020

INDICADOR:
Acompañamiento a la implementación del nuevo datacenter en la construcción del nuevo edificio del Concejo de Bogotá

OBSERVACIONES:

- En la gestión de los riesgos de Seguridad Digital no se evidenció el establecimiento del contexto externo e interno ni se actualizó el inventario de Activos de la Información.

- No se definieron en forma individual los riesgos pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

- No se observó la agrupación de activos del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

- Evaluación del Diseño de los Controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  Se definió un control con una calificación de 100.

  El control 1 mitiga parcialmente la causa raíz 1 porque no existe coherencia entre el control aplicado “Seguridad Física Ambiental” con la causa “Tuberías de desagüe que pasan por el Centro de Cableado” dado que en el Manual de Políticas 8.8.1.2.8 no se hace referencia específica al tema y por tanto, no se debió calificar el control con el máximo puntaje.

- Respecto al Plan de Tratamiento de Riesgos, el riesgo residual se calificó en Zona de Riesgo Alto y según la “Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019” el tratamiento es Reducir (se implementan controles).
  El proceso definió la actividad de control “Hacer acompañamiento a la implementación del datacenter en la construcción del nuevo edificio del Concejo de Bogotá D.C.” es un tema difícil de medir y no se puede evaluar su ejecución.
  No es un control apropiado porque no se identifica la segregación de funciones y por ende, no logra la reducción de riesgos.

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 6

Acceso indebido, hurto, manipulación o adulteración de la información para beneficio propio o de un tercero.

CLASIFICACIÓN DEL RIESGO

Corrupción

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
-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 2020

INDICADOR:
Número de actividades de sensibilización o divulgación realizadas

OBSERVACIONES:

- Se determinó el diligenciamiento de las 19 preguntas correspondientes a los Criterios parar calificar el impacto de Riesgos de Corrupción

- Evaluación del Diseño de los Controles:
  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:
  Se definieron dos controles donde cada uno obtuvo una calificación de 100, para un promedio de 100, con base en los criterios de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

  Control 1: mitiga parcialmente la causa raíz 1. Además, que se deriva del Procedimiento Realización de Copias de Seguridad Backup versión 9 de diciembre de 2018, el cual no fue actualizado en el 2019 con el fin de definir controles que cumpliera con todos los criterios que establece la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

  Control 2: no mitiga la causa raíz 2 y corresponde a una política de seguridad de la información que no cumple con todos los criterios de un control fuerte diseñado para mitigar el riesgo, por tal motivo, no se entiende porque se calificó con 100.

- Respecto al Plan de Tratamiento de Riesgos para el riesgo residual se calificó en Zona de Riesgo Moderado y el tratamiento elegido fue Evitar (se abandonan las actividades que dan lugar al riesgo). Sin embargo, el Proceso definió la actividad control relacionada con la "Sensibilización o divulgación de lo establecido en el Manual de políticas de seguridad de la información".

  Se observó que hubo un error en la selección del tratamiento porque se debió escoger Reducir en razón a que se va a ejecutar un control.

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 7

Obstaculización de un sistema informático del Concejo de Bogotá para beneficio propio o de un tercero

CLASIFICACIÓN DEL RIESGO
Corrupción

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
Realizar monitoreo de los sistemas de información.

SOPORTE:
Reporte generado por la plataforma de monitoreo

TIEMPO
Diciembre de 2020

INDICADOR:
Número de incidentes presentados

OBSERVACIONES:

- Se determinó el diligenciamiento de las 19 preguntas correspondientes a los Criterios parar calificar el impacto de Riesgos de Corrupción

- Evaluación del Diseño de los controles:

Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

El Proceso para este riesgo definió un control que alcanzó una calificación de 100. No obstante, mitiga parcialmente las causas 1 y 2.
Además, dicho control proviene del Procedimiento Administración y Actualización de la Red y Servidores, versión 7 de 2018, el cual no fue actualizado en el 2019.
El fin de la actualización era definir controles que cumplieran con todos los criterios que establece la Guía para la Administración del Riesgo y el Diseño de Controles
Por lo tanto, la calificación del diseño del control se considera Débil.

- Respecto al Plan de Tratamiento de Riesgos el riesgo residual se calificó en Zona de Riesgo Extremo y el Proceso seleccionó el tratamiento de Evitar (se abandonan las actividades que dan lugar al riesgo) opción que cumple con la "Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019". Sin embargo, el Proceso definió una actividad de control.

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 8

Inadecuada configuración de la infraestructura tecnológica de la Corporación

CLASIFICACIÓN DEL RIESGO

Riesgo Tecnológico

DESCRIPCIÓN DEL CONTROL:

Validación permanente por los profesionales del proceso de Sistemas, del soporte con los fabricantes o los representantes en el país de las herramientas tecnológicas.

PLAN DE TRATAMIENTO DE RIESGOS:

ACTIVIDAD DE CONTROL:

- Teniendo en cuenta el nivel del riesgo residual no se establecen actividades adicionales a los controles ya establecidos.

SOPORTE:

N.A.

TIEMPO

N.A.

INDICADOR:

N.A.

OBSERVACIONES:

- Evaluación del Diseño de los controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  El Proceso para este riesgo definió dos controles que lograron una calificación de 100. para un promedio de 100

  Los controles 1 y 2 mitigan parcialmente las causas 1 y 2 porque el Procedimiento de Administración y Actualización de la Red y Servidores versión 7 de diciembre de 2018, el cual no fue actualizado en el 2019 con el fin de definir controles que cumplieran con todos los criterios que establece la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

- Respecto al Plan de Tratamiento de Riesgos el riesgo residual se calificó en Zona de Riesgo Bajo y según la “Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019” el tratamiento es Aceptar (es decir, que no se adopta ninguna medida) pero de acuerdo con la guia se realiza seguimiento. Se observó que en el diligenciamiento de la Matriz de Riesgos no se escribió “Aceptar” sino “Asumir”

  Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RIESGO 9

Obsolescencia de la infraestructura tecnológica de la Corporación

CLASIFICACIÓN DEL RIESGO
Tecnológico

PLAN DE TRATAMIENTO DE RIESGOS:
ACTIVIDAD DE CONTROL:
Teniendo en cuenta el nivel del riesgo residual no se establecen actividades adicionales a los controles ya establecidos.

SOPORTE:
N.A.

TIEMPO
N.A.

INDICADOR:
N.A.

OBSERVACIONES:

- Evaluación del Diseño de los controles:

  Para la evaluación de los controles se tuvo en cuenta los siguientes aspectos: si definió responsable, su periodicidad, su propósito, como se realiza el control, las desviaciones producto de su ejecución y las evidencias de su ejecución. De esta labor se concluye:

  El Proceso para este riesgo definió dos controles, el control 1 alcanzó una calificación de 85 y el control 2 de 100, para un promedio de 92.5.
  Frente a este resultado, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas definió que: "Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96, se debe establecer un plan de acción que permita tener un control o controles bien diseñados"[3]. En consecuencia, el diseño del control es débil.

- Respecto al Plan de Tratamiento de Riesgos el riesgo residual se calificó en Zona de Riesgo Bajo y según la "*Guía de Política de Administración de Riesgo GMC-GU-002 del 18 de noviembre de 2019*" el tratamiento es Aceptar (es decir, que no se adopta ninguna medida) pero de acuerdo con la guia se realiza seguimiento.
  Se observó que en el diligenciamiento de la Matriz de Riesgos no se escribió "Aceptar" sino "Asumir".

[3] Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4. Octubre de 2018. DAFP. pág. 62

Es importante, resaltar que en los Lineamientos para la Gestión de Riesgos de Seguridad Digital establecen que se pueden utilizar los Objetivos de Control y Controles de Referencia establecidos del Anexo A de la Norma ISO/IEC 27001:2013). para el tratamiento de los riesgos inherentes.

RECOMENDACIONES –
Es necesaria la designación de un servidor público que lidere temas como revisión y actualización de procedimientos, manuales y políticas, la definición de los activos de información, la aplicación de la metodología de administración de riesgos, el seguimiento al plan de mejoramiento, el funcionamiento del Equipo Técnico de Seguridad de la Información, entre otros aspectos.
Además, que en el proceso de revisión y actualización se tengan en cuenta las no conformidades y oportunidades de mejora comunicadas.
Es importante trabajar en la cultura del seguimiento, análisis y evaluación que se encuentre debidamente documentada, para que contribuya a cumplir con las metas y objetivos del Proceso de SSI.
Así mismo, es imprescindible trabajar en la implementación del Manual de Gobierno Digital en la Corporación.

CONCLUSIONES -
Realizada la auditoría al Proceso de Sistemas y Seguridad de la Información se concluye que las No Conformidades comunicadas son producto de la desactualización de los procedimientos y políticas de seguridad, las falencias en la aplicación de la metodología de riesgos, así como, las debilidades en el monitoreo y seguimiento de las actividades a cargo del Proceso.

AUDITOR LÍDER	
Nidia Cano Sánchez	Firma (s):
EQUIPO AUDITOR	
Nombre:	Firma (s):

JEFE OFICINA DE CONTROL INTERNO	
Aura María Carrillo Vargas	Firma:
FECHA DE ENTREGA	17/07/2020