REPÚBLICA DE COLOMBIA

CONCEJO DE BOGOTA 10-05-2019 11:47:24
Al Contestar Cite Este Nr.:2019IE6719 O 1 Fol:1 Anex:10
CONTROL INTERNO/CHAVERRA OVALLE HITLER ROUSEAU
DIRECCION ADMINISTRATIVA/SANDOVAL AVILA NANCY ADR
REMISION INFORME FINAL AUDITORIA INTERNA
SISTEMAS

CONCEJO DE BOGOTÁ, D.C.

MEMORANDO

PARA: Dra. NANCY ADRIANA SANDOVAL AVILA
Directora Administrativa

DE: Jefe Oficina de Control Interno

ASUNTO: Remisión Informe Final Auditoria Interna

En cumplimiento de la función evaluadora asignada a la Oficina de Control Interno en la normatividad vigente, de manera atenta, nos permitimos hacer entrega del informe final de la Auditoría realizada al proceso de Sistemas y Seguridad de la Información, juntamente con el seguimiento a los Planes de Mejoramiento.

Así mismo, para que la recepción del plan de mejoramiento no presente contratiempos, se les recuerda allegar a más tardar diez días hábiles al recibo de la presente comunicación lo siguiente, de acuerdo al procedimiento EI-PR001:

- Plan De Mejoramiento con la Formulación de las Acciones Correctivas y Preventivas Formato SIG-PR007FO1.
- Acta de Reunión de los funcionarios adscritos al proceso para la formulación de las acciones.
- Acta de Reunión con los funcionarios de la Oficina Asesora de Planeación para el asesoramiento para la formulación de las acciones.
- Copia de las acciones correctivas y preventivas en formato digital editable.

Es importante recordar que la formulación del Plan de Mejoramiento se realiza sobre el numeral 10.2 del Informe Definitivo, igualmente es necesario realizarlo en conjunto con los responsables de cada procedimiento y sus funcionarios, con el fin de involucrar a todo el equipo en el cumplimiento del mismo.

Cordialmente,

HITLER ROUSEAU CHAVERRA OVALLE

Anexo lo anunciado en diez folios

Proyectó: Marcel Pedraza Avila, Secretario Ejecutivo 425-05

10-V-2019
3p

1. INFORME DEFINITIVO DE AUDITORÍA

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

2. OBJETO

Determinar el grado de cumplimiento de los requisitos de la Norma ISO 27001:2013, así como el acatamiento de los requisitos legales, reglamentarios y la documentación establecida por la Corporación.

3. ALCANCE DE LA AUDITORÍA

El Subsistema de Gestión de Seguridad de la Información (SGSI) del Concejo de Bogotá D.C., cuya sede principal está ubicada en la Calle 36 No. 28 A 41 de la ciudad de Bogotá y los datacenter ubicados en el segundo piso de la Carrera 30 No. 25 – 90, abarca el proceso de Sistemas y Seguridad de la Información y los procesos misionales de la Corporación, que son:

1. Control Político.
2. Gestión Normativa.
3. Elección de Servidores Públicos Distritales.
4. Atención al Ciudadano.

4. CRITERIOS AUDITORÍA

ISO 27001:2013 Norma Técnica de Gestión de Seguridad de la Información.
Manuales, Procedimientos, Planes de Acción, Políticas de Operación, Planes de Mejoramiento, Aplicativos y Normas Legales que le apliquen al proceso.
Ley 87 de 1993."*Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones*"
Ley 80 de 1993 "*Por la cual se expide el Estatuto General de Contratación de la Administración Pública*" y sus reglamentarias.
Decreto 103 de 2015 "*Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*"
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.*"

5. RESPONSABLE /PROCESO/ DEPENDENCIA

Nancy Adriana Sandoval Ávila – Directora Administrativa.

6. EQUIPO AUDITOR

Dr. Hitler Rousseau Chaverra Ovalle (Jefe Oficina de Control Interno).
Nidia Cano Sánchez - Auditor Líder.
Sorel Velásquez Quintero.
Diego Andrés Lemus Rodríguez.
Luis Argenio Mariño Roa.

7. AUDITADOS

Diana Ávila Pinzón - Oficina Asesora de Planeación.
Francisco Bernal, Carlos Muñoz - Proceso Sistemas y Seguridad de la Información.
Yolanda Canchilla Quintero – Fondo Cuenta.

Reinaldo García Baquero – Atención a la Ciudadanía
Tulia Niño Martínez y Rosa Elena Morales - Gestión Normativa
Hernán Rodríguez Mora – Gestión Documental

8. METODOLOGÍA

Se realizó reunión de apertura el 1 de abril de 2019, dando lectura al Plan de la auditoría, con el siguiente contenido: 1. Apertura de la auditoría - presentación de los integrantes del equipo auditor. 2. Objetivo de la auditoría. 3. Alcance y criterios de la Auditoría. 4. Áreas a visitar 5. Tratamiento de no conformidades y oportunidades de mejora identificadas en la auditoría. 6. Informe Preliminar 7. Reunión de cierre.

Teniendo en cuenta que la Directora Administrativa y el responsable del proceso de Seguridad de la Información en el momento del inicio de la auditoría se encontraban en entrega y recibo de sus cargos, se inició la auditoría con la aplicación de la lista de chequeo a las otras áreas seleccionadas en el Plan de Auditoría, además se verificó la documentación del proceso que estaba publicada en la red interna, INTRANET.

9. PERÍODO DE EJECUCIÓN DE LA AUDITORÍA

1 de abril al 9 de mayo de 2019.

10. HALLAZGOS

En desarrollo de la auditoría al proceso y los procedimientos se encontraron los siguientes hallazgos:

10.1 CONFORMIDADES

En la evaluación del Sistema de Gestión de Seguridad de la Información se determinaron las siguientes fortalezas:
El proceso cuenta con personal calificado y de planta para el desarrollo de sus labores.
Se elaboró el documento de identificación de las partes interesadas.
Se dispone de un procedimiento de seguridad perimetral.
Se realiza un control de roles de acceso a la red.
El Sistema cuenta con un control para la instalación de software.
Existe una política de segmentación de redes.
En el año 2018 se adquirieron nuevos computadores para la Corporación.

10.2 NO CONFORMIDADES

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*"

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 debe 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 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.

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 que el inventario de los activos de información se encuentra incompleto y desactualizado.

También se observó que en los documentos del Proceso de Sistemas y Seguridad de la Información en la carpeta 7, denominada Gestión de Riesgos se encuentra el subdirectorio 1. Documentación el "*Instructivo Gestión de Riesgos de Seguridad de la Información*", donde se explica la matriz de riesgos del Sistema de Seguridad, el cual no fue adoptado como un documento oficial del Sistema Integrado de Gestión (SIG) de la Corporación.

Lo anteriormente descrito, vulnera lo definido en el numeral 6.1.2 "*Valoración de Riesgos de la Seguridad de la Información*" literal c. Identifique los riesgos d. Analice los riesgos e. Evalué los riesgos y el numeral 8.2 "*Evaluación de Riesgos de Seguridad de la Información*" de la Norma ISO 27001:2013 Sistema de Gestión de Seguridad de la Información; así mismo, se incumple el numeral 10 "*Participar en la formulación y evaluación de los planes de acción para mitigar y/o asumir riesgos de seguridad de la información*" 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*".

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*".

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.

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 el 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.

10.2.7. Se evidenció que pese a que la Corporación utiliza el aplicativo CORDIS, su funcionalidad no es la adecuada, debido a que el inicio del procedimiento se estampa sello de caucho como prueba de radicación de la correspondencia y en forma posterior se ingresa al aplicativo para generar el número de radicación y escanear los anexos. Lo que representa un riesgo de pérdida de documentos, errores en la transcripción y dificultad para efectuar el seguimiento de su gestión; situación que incumple lo establecido en el literal c. "*Identifique los riesgos de la seguridad de la información*" del numeral 6.1.2. Valoración de riesgos de Seguridad de la Información de la Norma ISO 27001:2013.

10.2.8. Los elementos de Hardware y Software son activos de la Corporación, de conformidad con los numerales 8.5.3.1 y 8.5.3.4.3 del Manual de Políticas de seguridad de la información del Concejo de Bogotá. 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.

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.

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.

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.

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.

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.

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.

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…*".

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.
Adicionalmente, pese a que en el numeral 2 Asuntos Contractuales, literal c del texto del Convenio se contempla la figura jurídica de la delegación, ésta no sustenta debidamente la delegación por parte de los representantes legales de las entidades a funcionarios de menor jerarquía para que puedan suscribir convenios. Lo anterior indica que éste soporte no es un documento con todas las exigencias legales.

Hecho que transgrede los artículos 2.2.1.2.1.4.1. "*Acto administrativo de justificación de la contratación directa*", 2.2.1.2.1.4.4. "*Convenios o contratos interadministrativos*" del Decreto 1082 de 2015, así como, el artículo 40 "*Del Contenido del Contrato Estatal*" de la ley 80 de 1993. Además, se incumplen los literales 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*" y e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*" del artículo 2º de la ley 87 de 1993.

10.3 OPORTUNIDADES DE MEJORA

- Al analizar el Mapa de Procesos de la Corporación, se observa que el proceso Gestión Sistemas de Información se encuentra clasificado como de apoyo y está a cargo de la Dirección Administrativa; cuando la naturaleza e importancia de la información para los grupos de interés requieren un Sistema más robusto, dinámico y seguro; situación que amerita estudiar un ajuste en su clasificación como

estratégico y que las decisiones que tome la alta dirección aseguren la mejora continua.

- Se recomienda la actualización del Formato en el que se presenta el Manual de Políticas de Seguridad (versión 3 de 10 de mayo de 2018), debido a que no corresponde al vigente. Es decir, se debe eliminar el logo de OSHAS.
- Se recomienda que se instale una cámara al interior de las zonas de acceso restringido, con el propósito de controlar las actividades de las personas que ingresan a dichas zonas.
- La información relacionada con el proceso de Sistemas de Gestión de Seguridad de la Información se encuentra publicada en varias carpetas de la red interna, dificultando su consulta, aplicabilidad y control; por ende, se recomienda su revisión y ubicarla en una sola carpeta de la red interna.
- Se determinó que en la cintoteca ubicada en el segundo piso de la sede de SDH no existe un detector de humo y por ello se recomienda instalarlo, para mejorar la seguridad del lugar.
- Se recomienda que se actualice la versión del aplicativo PERNO (Manejo Sistematizado del Recurso Humano) que se utiliza en la Corporación a través de la Secretaría Distrital de Hacienda.
- Se evidenció que diversas áreas del Concejo de Bogotá D.C. perciben las políticas de seguridad como muy restrictivas para el desarrollo de sus labores y por ello se recomienda realizar una revisión del Manual de Políticas para adaptarlas a la estructura y necesidades de la Corporación.
- Respecto al Plan de Continuidad se recomienda que a todos los directivos se les socialice sobre los roles y responsabilidades que tienen asignados frente a una posible crisis, dado el alto grado de rotación de los mismos.
- Se establecieron deficiencias en la capacitación y concientización a la entidad sobre el Sistema de Seguridad de la Información, sus políticas y procedimientos transversales, por lo tanto se recomienda implementar un plan de capacitación que contribuya a la apropiación de la importancia de este Sistema para el adecuado desarrollo de las labores en la Corporación.
-

11. CONCLUSIONES

Realizada la auditoría al Sistema de Gestión de Seguridad de la Información se concluye que la mayoría de No Conformidades observadas son resultado de la desactualización del inventario de activos de información y de los riesgos, así como, de las falencias en la aplicación de las políticas y procedimientos establecidos. Lo que se originó en falta de capacitación y concientización sobre el Sistema de Seguridad de la Información y su respectivo monitoreo, seguimiento, análisis y evaluación en cumplimiento de los roles establecidos a los diferentes actores que tienen relación con el Sistema.

12. RECOMENDACIONES

Es importante que el Proceso de Sistemas y Seguridad de la Información actualice sus políticas y procedimientos en forma articulada con los demás componentes del SGSI y con los procesos de la Corporación, ajustándolos a la realidad institucional y teniendo en cuenta las no conformidades y oportunidades de mejora comunicadas.
Así mismo, es fundamental trabajar en la cultura del seguimiento, análisis y evaluación (debidamente soportada), que permita tomar medidas oportunas para evitar desviaciones y lograr cumplir las metas y objetivos del SGSI.

AUDITOR LIDER	
Nombre: Nidia Cano Sánchez	Firma: Nidia S

JEFE OFICINA DE CONTROL INTERNO	
Nombre : Hitler Rosseau Chaverra Ovalle	Firma:

FECHA DE ENTREGA	9 de mayo de 2019