

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 1 DE 13

Proceso:	Sistemas y Seguridad de la Información.
Líder del proceso/Jefe de dependencia:	Dr. Fernando Mantilla Ortiz Director Administrativo
Objeto:	Analizar y evaluar la información y establecer posibles no conformidades y oportunidades de mejora identificadas en el proceso de sistemas y seguridad de la información de la corporación.
Alcance:	<p>Evaluar la gestión del proceso de sistemas y seguridad de la información de la Dirección Administrativa del Concejo de Bogotá, de manera posterior y selectiva, para la vigencia fiscal 2021, mediante la aplicación simultánea y articulada de los procedimientos establecidos por la entidad y el seguimiento al plan de mejoramiento; de tal forma que permita opinar sobre la gestión del proceso de sistemas y la calidad y, eficiencia del mismo.</p> <p>Es importante, destacar que en la vigencia 2021 la Corporación no realizó Auditoría Interna al Proceso, debido a la no disposición de personal técnico especializado en esta materia de auditoría y la aprobación en el Comité Institucional de Coordinación de Control Interno efectuado el 15 de septiembre de 2021, donde en el punto 7 del citado Comité, se presentó la reformulación del Programa Anual de Auditorías y la reformulación de acciones del proceso para la vigencia.</p>
Criterios:	<ul style="list-style-type: none"> • Resolución 1519 de 2020 del Min Tic <i>“Por la cual se definen los estándares y directrices para publicar la información señalada en la ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”</i> • Ley 1581 de 2012, ley de habeas data 1266 de 2008 y el decreto 1377 de 2013. • Ley 1712/2014, 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. • Decreto 1008/2018 "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" • Decreto 1083 de 2015, por el cual se expedición el decreto único reglamentario del sector de la función pública. (adiciones y modificaciones) • Resolución número 00500 de marzo 10 de 2021 <i>“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital”</i>

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 2 DE 13

	<ul style="list-style-type: none"> • Resolución 100 de 2021, “<i>Por la cual se adopta la política de riesgos en el concejo de Bogotá D.C.</i>” • Resolución No. 028 del 2021 “<i>Por medio de la cual se adopta el plan de acción para la vigencia 2021</i>”. • Resolución 343 de 2020 “<i>Por el cual se expide el plan cuatrienal para el concejo de Bogotá 2020 - 2023</i>” • Resolución 066/2022 • NTC 5854– accesibilidad web planes de mejoramiento • Manual de gobierno digital • Modelo nacional de gestión de riesgos de seguridad digital 	
Equipo Auditor:	Yeisonn Alexander Chipatecua Quevedo, Ingeniero de Sistemas Contratista – Nidia Cano Sánchez, Profesional Especializado 222-05.	
Auditados:	Dr. Fernando Mantilla Ortiz Director Administrativo Ing. Francisco Bernal- Profesional Especializado 222-04, Asignado al Proceso de Sistemas y Seguridad de la Información	
Metodología:	<p>Se destaca la buena disposición para la atención de la auditoría interna por parte de las áreas y funcionarios auditados, el apoyo logístico de la Oficina de Control Interno y la Dirección Administrativa en particular los funcionarios encargados del proceso de Sistemas y Seguridad de la Información.</p> <p>Se realizó reunión de apertura el 03 de Marzo 2022, 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. Calendario de la auditoría 5. Reunión de cierre.</p> <p>A continuación, un resumen de la metodología de la ejecución del plan de auditoría interna al Proceso de sistemas y seguridad de la información del concejo de Bogotá., bajo la NTC/ISO 27001:2013 y el modelo COBIT, para ello se van a revisar individualmente el cumplimiento y desarrollo de los 13 procedimientos asociados al proceso y los requerimientos de Norma NTC/ISO 27001:2013 repartidos en 7 numerales, y 114 controles del Anexo A, correspondientes a 14 dominios de control. La auditoría se realizó con la participación de los responsables del proceso.</p>	
Fechas de Ejecución de la Auditoría:	Desde (día/mes/año):	03/03/2022
	Hasta (día/mes/año):	01/08/2022
Reunión de Cierre:	(día/mes/año)	18/07/2022

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 3 DE 13

<p>I. PROCEDIMIENTOS PROCESO DE SISTEMAS Y SEGURIDAD DE LA INFOMACIÓN</p> <p>1. CONFORMIDADES:</p> <p>1.1. Se determinó la aplicación del procedimiento Administración y Actualización de Red y Servidores, dando alcance a su objetivo en asegurar la correcta operación de la red y servidores. Y como muestra de auditoria se pudo verificar la prestación del servicio ágil, eficiente, monitoreado y seguro de calidad a los usuarios.</p> <p>1.2. La Oficina de Control Interno, estableció la aplicación del procedimiento Realización de Copias de Seguridad backup, dando cumplimiento a su objeto en el cual garantiza el aseguramiento de la información institucional digital creada, procesada y almacenada; haciendo uso de los sistemas y servicios informáticos misionales y administrativos del Concejo de Bogotá D.C., mediante las copias de seguridad.</p> <p>1.3. Se estableció que, el procedimiento de Soporte Tecnológico, realizó la atención de incidentes y requerimientos de forma adecuada, tenido en cuenta los niveles de servicios establecidos por la entidad.</p> <p>1.4. De igual forma, dentro de la auditoría realizada se verificó que para el procedimiento Administración de Equipos de Cóputos, la administración garantiza que la plataforma tecnológica asignada para los funcionarios del Concejo de Bogotá, se encuentra en funcionamiento en todo momento.</p> <p>1.5. Así mismo se verificó que para el procedimiento Gestión de la Capacidad, se establecieron lineamientos para asegurar que se cubran las necesidades de capacidad en la infraestructura tecnológica del Concejo de Bogotá.</p> <p>1.6. Dentro de las preguntas realizadas al procedimiento de Clasificación, Etiquetado y manejo de Información, se verificó que la Dirección proporciona las directrices para un adecuado etiquetado y manejo de información física y digital en cumplimiento de los requisitos NTC/ISO 27001:2013 y la Ley 1712 de 2014.</p> <p>1.7. Dado lo anterior, y dentro del procedimiento de Gestión de Cambios, se verificó que establecieron las actividades necesarias para gestionar de manera correcta los cambios requeridos en sistemas de la información y en general la infraestructura tecnológica (se pasó de tecnología análoga y digital a telefonía IP), para la Corporación.</p> <p>1.8. Con relación a la aplicación del procedimiento de Continuidad del Negocio, este auditor verificó que, ante situaciones de fallas o desastres, la Administración ha avanzado la capacidad de respuestas ante esta situación y así poder darle continuidad al proceso de sistemas y seguridad de la información.</p> <p>2. NO CONFORMIDADES:</p> <p>2.1 Se evidenció, que el procedimiento “Realización de copias de seguridad backup”, numeral 6.8. “El Auxiliar Administrativo marca las cintas de forma organizada con los parámetros de</p>
--

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 4 DE 13

almacenamiento entregados por el Profesional Universitario como lo es: Fecha del backup, nombre del servidor y nombre de trabajo de Backup y se almacenan en cintoteca”, no es realizada por el auxiliar administrativo según respuesta entregada por la Dirección, en donde indican que: “La marcación de cintas no se está realizando por parte del el Auxiliar Administrativo; toda vez, el proceso de SSI no cuenta con este recurso asignado. Esta actividad la realiza el profesional universitario”.

Se determinó que el numeral 6.9, *“El Auxiliar Administrativo registra en la bitácora de copias de seguridad el Tipo de Sesión, Esp, Estado, Modo Backup, Total Incremental, Tiempo de Inicio, En cola, Duración, GB Escritos, N° Cintas, N° Errores, N° Advertencias, N° Archivos, Avance y ID de la Sesión; según formato (SSI-PR002-FO1) el cual se lleva en formato Excel y de forma local en equipo”.* Tampoco es desarrollada por un auxiliar administrativo dado que, en su respuesta indicaron: *“Por cuanto no se cuenta con este recurso, la actividad del registro en la bitácora, la está haciendo el Profesional Universitario”.*

Tanto el numeral 6.8 y 6.9, son resultado de la falta de la Revisión y Actualización del Procedimiento, porque lleva a no ejecutarse de acuerdo a la descripción del mismo.

Se incumple el literal b. Garantizar la eficacia, la eficiencia y economía en todas las operaciones promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional; del artículo 2° de la ley 87 de 1993.

Analizada la respuesta entregada, no está direccionada a desvirtuar el fundamento de la NO CONFORMIDAD, toda vez que la entidad debe actualizar el procedimiento para definir el personal idóneo para realizan las actividades citadas.

Por lo tanto, no se acepta la respuesta a esta No Conformidad y se ratifica para ser incluida en el Plan de Mejoramiento.

2.2. Dentro del procedimiento *“Atención de soporte tecnológico”*, se pudo verificar que la entidad no cuenta con un plan de mantenimiento como lo indica el numeral 6.6. Informes y estadísticas *“El contrato de mesa de ayuda debe contar con un plan de mantenimiento (Planilla Mantenimiento Preventivo Equipo – SSI-PR003-FO2), el cual debe ser revisado y aprobado por el encargado del proceso de Sistemas y Seguridad de la Información”.*

Analizada la respuesta por la Dirección, indicando que *“El contrato de mesa de servicios incluye los mantenimientos preventivos, y tanto el procedimiento como el formato se encuentran en revisión para ser actualizados, los mantenimientos se registran en un formato acordado con el contratista de mesa de servicios que contiene mucha más información”.*

Se incumple el literal h. *“Velar porque la entidad disponga de procesos de planeación y mecanismos adecuados para el diseño y desarrollo organizacional, de acuerdo con su naturaleza y características”* del Artículo 2° de la ley 87 de 1993.

Dado lo anterior se debe realizar un plan de mantenimiento que contenga todo lo relacionado con procedimiento de atención de soporte tecnológico.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 5 DE 13

Por lo tanto, no se acepta la respuesta a esta No Conformidad y se ratifica para ser incluida en el Plan de Mejoramiento.

3. OPORTUNIDADES DE MEJORA:

3.1. Se observó que el responsable de determinar el nivel de prioridad del incidente es el Oficial de Seguridad de conformidad con el procedimiento SSI-PR007, la actividad no tiene continuidad debido a que el oficial o responsable de seguridad de la información no se encuentra vinculado a la Corporación. En consecuencia, muchos incidentes pasan a ser resueltos por el equipo de profesionales del proceso en búsqueda del restablecimiento de los servicios en el menor tiempo posible, se recomienda vincular al Oficial de Seguridad de forma permanente y así no generar traumatismos internos del proceso.

3.2. Teniendo en cuenta que si la evaluación final determina que el proceso y los resultados han sido satisfactorios se procede al cierre del cambio por parte del Líder de Cambios. Adicionalmente, se debe comunicar a las partes interesadas (involucradas en el cambio) la finalización del mismo, es necesario nombrar un líder de cambios como lo plasma el procedimiento.

VERIFICACIÓN DE PLANES DE MEJORAMIENTO DERIVADOS DE AUDITORÍAS ANTERIORES

INFORME FINAL DE AUDITORIA INTERNA PROCESO DE SSI VIGENCIA 2020

NO CONFORMIDAD 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 2° Objetivos del Sistema de Control Interno de la ley 87 de 1993.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 6 DE 13

ACCION PROPUESTA.

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

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO.

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.

CONCLUSIÓN.

Se establece con relación a la respuesta del seguimiento de la acción, los hechos que dieron origen a la observación aún siguen vigentes y sigue calificada como abierta.

NO CONFORMIDAD 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 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.

ACCION PROPUESTA:

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

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO:

De la respuesta del Proceso de SSI se destaca: “Se viene trabajando en la actualización de los procedimientos adscritos al proceso de sistemas y seguridad de la información... en la actualidad el estado de la actualización de los procedimientos es el siguiente:

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 7 DE 13

Código	Procedimiento	Encargado	Estado
SSI-PR001	Administración y actualización de la Red y Servidores	Luis Argenio Mariño Roa	En proceso de actualización
SSI-PR002	Realización de Copias de Seguridad Backup	Luis Argenio Mariño Roa	En proceso de actualización
SSI-PR003	Atención de Soporte Tecnológico	Francisco Alfonso Naranjo Madero	En proceso de actualización
SSI-PR004	Administración Equipos de Cómputo	Francisco Javier Bernal García	En proceso de actualización
SSI-PR005	Plan de Necesidades de Contratación y Seguimiento a los contratos de Tecnología	Francisco Javier Bernal García	En proceso de actualización
SSI-PR006	Gestión de la Capacidad	Luis Argenio Mariño Roa	Por actualizar
SSI-PR007	Gestión de Incidentes de Seguridad de la Información	Diego Andrés Lemus Rodríguez	En proceso de actualización
SSI-PR008	Clasificación, etiquetado y manejo de la Información	Francisco Alfonso Naranjo Madero	Por actualizar
SSI-PR009	Acceso físico a las Instalaciones e Ingreso Equipos portátiles	Diego Andrés Lemus Rodríguez	Trasladado al proceso de Recursos Físicos
SSI-PR010	Acceso Lógico	Francisco Alfonso Naranjo Madero	Actualizado y enviado a la OAP
SSI-PR011	Gestión de Activos	Francisco Javier Bernal García	Por actualizar
SSI-PR012	Gestión de Cambios	Diego Andrés Lemus Rodríguez	Por actualizar
SSI-PR013	Procedimiento Continuidad de Negocio	Francisco Javier Bernal García y Francisco Alfonso Naranjo Madero	Actualizado en Octubre de 2021

Se establece con relación a la respuesta del seguimiento de la acción, los hechos que dieron origen a la observación aún se encuentran vigentes, es decir que el Proceso de Sistemas y Seguridad de la Información **no actualizó 12 procedimientos** (como se puede observar en el cuadro anterior), en los años 2019, 2020 y 2021. Con relación al procedimiento SSI-PR013 fue actualizado en el 2021 por el Proceso SSI.

CONCLUSIÓN.-

La acción se califica como abierta para los 12 procedimientos del Proceso de Sistemas y Seguridad de la Información que, no han sido actualizados.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 8 DE 13

NO CONFORMIDAD 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 identificada 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.

ACCION PROPUESTA.-

Se realizará en conjunto con la Oficina Asesora de Planeación la revisión de la Política de Administración de Riesgos del Concejo de Bogotá para definir si se realiza 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. Para esto se solicitará el acompañamiento de la Oficina de Control Interno.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO:

El Proceso de SSI informó: “*Se viene trabajando en conjunto con la Oficina Asesora de Planeación la revisión de la Política de Administración de Riesgos del Concejo de Bogotá dado que esta oficina es quien publica la misma, desde el proceso de Sistemas y Seguridad de la Información se ha remitido la información pertinente con el fin de ajustar dicha política y que se realicen los ajustes a la nueva versión*”.

CONCLUSIÓN.

En cuanto a esta respuesta, mientras no se realice el ajuste y actualización continua la acción abierta.

NO CONFORMIDAD 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.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 9 DE 13

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.

ACCION PROPUESTA.

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 realizarán los ajustes pertinentes que le correspondan al proceso.

SEGUIMIENTO DE LA OFICINA DE CONTROL INTERNO:

El Proceso de SSI respondió: "*Se viene trabajando en conjunto con la Oficina Asesora de Planeación la revisión de la Política de Administración de Riesgos del Concejo de Bogotá dado que esta oficina es quien publica la misma, desde el proceso de Sistemas y Seguridad de la Información se ha remitido la información pertinente con el fin de ajustar dicha política y que se realicen los ajustes en la nueva versión*".

CONCLUSIÓN:

En cuanto a esta respuesta, mientras no se realice el ajuste y actualización la acción continúa abierta

2. SEGUIMIENTO MATRIZ DE RIESGOS Y ANALISIS DE CONTROLES

RIESGO 1. Acceso indebido, hurto, manipulación o adulteración de la información para beneficio propio o de un tercero.

CLASIFICACIÓN DE RIESGO: Corrupción

ACTIVIDAD DE CONTROL:

- El Sistema de copias de seguridad, diariamente genera una copia de respaldo de la información en otro medio, el profesional asignado verifica, que se haya realizado correctamente, de encontrarse inconsistencias se detecta la causa y se genera nuevamente el back up.

- Cada servidor público del Concejo de Bogotá D.C de forma permanente da cumplimiento del Manual de Políticas de seguridad de la información. Verifica que hace uso correcto a los sistemas a su cargo. Cuando se presenten fallas solicita la presencia de la mesa de ayuda. En caso de no dar cumplimiento al Manual, se llevan a cabo las acciones disciplinarias a que se dé lugar

PLAN DE TRATAMIENTO DE RIESGOS:

Sensibilización o divulgación de lo establecido en el Manual de políticas de seguridad de la información.

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 10 DE 13

SOPORTE:

Evidencias de las actividades realizadas (Correos con las divulgaciones, fotos y registros de asistencias, entre otras)

TIEMPO:

Diciembre 2022

INDICADOR: N.A.

OBSERVACIONES:

Se observa que el plan de tratamiento está en construcción y hace parte del plan de mejoramiento del proceso ya que depende exclusivamente de la capacidad técnica del Oficial de Seguridad encargado

RIESGO 2. Obstaculización de un sistema informático del Concejo de Bogotá para beneficio propio o de un tercero

CLASIFICACIÓN DE RIESGO:

Corrupción

ACTIVIDAD DE CONTROL:

El responsable de cada sistema verifica, de forma permanente que los sistemas estén actualizados a la versión más estable del fabricante o proveedor. En caso de no poder actualizar los sistemas se aplican controles alternos.

PLAN DE TRATAMIENTO DE RIESGOS:

Realizar monitoreo de los sistemas de información.

SOPORTE:

Reporte generado por la plataforma de monitoreo

TIEMPO:

Diciembre 2022

INDICADOR: N.A.

OBSERVACIONES:

Se observa que el plan de tratamiento previene una de las causas

RIESGO 3: Inadecuada configuración de la infraestructura tecnológica de la Corporación

CLASIFICACIÓN DE RIESGO:

Tecnológicos

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 11 DE 13

ACTIVIDAD DE CONTROL:

- Los profesionales del proceso de Sistemas, validan permanentemente el soporte con los fabricantes o los representantes en el país de las herramientas tecnológicas.

- El equipo de Sistemas y Seguridad de la Información, verifica que los proveedores o fabricantes realicen la transferencia de conocimiento a los funcionarios de SSI sobre el manejo de las herramientas, dependiendo de las necesidades. De no hacerse en los tiempos requeridos se solicita mediante comunicación el cumplimiento de los compromisos para no afectar la operación de la Corporación.

PLAN DE TRATAMIENTO DE RIESGOS: N/A

Teniendo en cuenta el nivel del riesgo residual está en zona baja, no se establecen actividades adicionales a los controles ya establecidos

SOPORTE: N/A

TIEMPO: N/A

INDICADOR: N/A

OBSERVACIONES: N/A

RIESGO 4: Obsolescencia de la infraestructura tecnológica de la Corporación

CLASIFICACIÓN DE RIESGO:

Tecnológicos

ACTIVIDAD DE CONTROL:

- El equipo de Sistemas y Seguridad de la Información, verifica de forma regular las necesidades de actualización de los sistemas, de acuerdo a los requerimientos y realiza la gestión para hacer las solicitudes de recursos que permitan contar con las inversiones requeridas. Las solicitudes se consolidan en las correspondientes fichas técnicas y solicitudes de contratación.

- Los profesionales del proceso de Sistemas y Seguridad de la Información de acuerdo al cronograma de contratación, verifican y gestionan los contratos de soporte para la actualización o renovación de la infraestructura tecnológica. Las solicitudes se diligencian en las fichas técnicas y solicitudes de contratación.

PLAN DE TRATAMIENTO DE RIESGOS:

Teniendo en cuenta el nivel del riesgo residual está en zona baja, no se establecen actividades adicionales a los controles ya establecidos

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 12 DE 13

SOPORTE: N/A

TIEMPO: N/A

INDICADOR: N/A

OBSERVACIONES: N/A

RECOMENDACIONES.

- Mantener el compromiso de la Dirección Administrativa, con el mejoramiento continuo de la gestión del proceso de sistemas y seguridad de la información y con el cumplimiento de las regulaciones y normas relacionadas con el fortalecimiento de la gestión TIC del sector público.
- Analizar, priorizar e implementar las acciones necesarias que realicen las oportunidades de mejora identificadas y las de los informes de los proveedores y encargados del proceso de sistemas y seguridad de la información sobre planes de seguridad informática, gestión de vulnerabilidades operativas, disponibilidad de dispositivos de seguridad, gestión de identidad y acceso, y cumplimiento del modelo operativo y del plan de actualización tecnológica, con el fin de prevenir daños por potenciales amenazas, de forma que se eviten no conformidades en el futuro.

CONCLUSIONES:

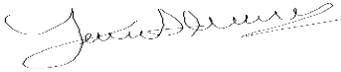
Evaluado el proceso de sistemas y seguridad de la Información, se concluye que:

- Existe una fuerte gestión tecnológica de la información, con énfasis en la seguridad informática, basada en medios y tecnología de punta, que le ha permitido al Concejo de Bogotá responder (en mayor medida y con seguridad razonable) a los retos y amenazas actuales del entorno.
- El proceso de sistemas y seguridad de la Información está en su fase de actualización, en consonancia con el Sistema Integrado de Gestión – SIG y el Modelo integrado de Planeación y Gestión – MIPG v 4, convirtiéndose en una herramienta de apoyo en la organización de procesos, controles y salvaguardas con los que se mantiene la información bajo medidas de seguridad para garantizar su integridad, confidencialidad, autenticidad y disponibilidad.
- Se evidencia el avance en la implementación de controles definidos para el proceso de sistemas y seguridad de la Información, sin embargo, se observan las oportunidades de mejora ya citadas, en cuanto a: documentación, procedimiento, mapa de riesgos y controles del sistema, las cuales requieren ser gestionadas.
- Procede fortalecer los mecanismos metodológicos internos de valoración y tratamiento de riesgos de seguridad de la información, con el fin de ser concordantes e integrados al sistema

 CONCEJO DE BOGOTÁ, D.C.	PROCESO EVALUACIÓN INDEPENDIENTE	CÓDIGO: EVI-FO-009
	INFORME FINAL DE AUDITORÍA	VERSIÓN: 07
		VIGENCIA: 20-Dic-2019
		PÁGINA 13 DE 13

general de riesgos, pues son la base fundamental de los sistemas de gestión que el Concejo de Bogotá adopta.

- Es importante evaluar la declaración de aplicabilidad de los controles de seguridad de la información de la entidad como parte del proceso de sistemas y seguridad de la Información, para definir los mecanismos de control a implementar.

AUDITOR LIDER	
Nombre: Yeisonn Alexander Chipatecua Quevedo	Firma (s): 
EQUIPO AUDITOR	
Nombre (s): Nidia Cano Sánchez Profesional Especializada	Firma (s): <i>Nidia Cano Sánchez</i>
JEFE OFICINA DE CONTROL INTERNO	
Nombre : Gloria María Gómez Cardona	Firma:  Firmado digitalmente por Gloria María Gómez Cardona
FECHA DE ENTREGA	6 septiembre 2022