REPÚBLICA DE COLOMBIA

CONCEJO DE BOGOTA 10-07-2017 03:11:46
Al Contestar Cite Este Nr.:2017IE9459 O 1 Fol:1 Anex:50
CONTROL INTERNO/PEÑA NIÑO EDWIN ANDERSON
DIRECCION ADMINISTRATIVA/ZAMBRANO OCAMPO GLORIA V
REMISION INFORMES FINALES AUDITORIA
TALENTO HUMANO, RECURSOS FISICOS, SISTEMAS

CONCEJO DE BOGOTÁ, D.C.

MEMORANDO

PARA: Doctora GLORIA VERONICA ZAMBRANO OCAMPO
Directora Administrativa

DE: Jefe Oficina de Control Interno

ASUNTO: Remisión Informes Finales 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 a los procesos de Talento Humano, Recursos Físicos y Sistemas y Seguridad de la Información.

Los informes anteriormente descritos varían en algunos de sus numerales al Informe Preliminar debido al ajuste de las evidencias presentadas por la Dirección Administrativa; los mismos contienen las fortalezas y hallazgos o no conformidades correspondientes.

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 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.

13 JUL 2017 4:55 p

REPÚBLICA DE COLOMBIA

CONCEJO DE BOGOTÁ, D.C.

Cordialmente,

EDWIN ANDERSON PEÑA NIÑO

Anexo: Lo anunciado. en 52 folios

1. INFORME REALIZACIÓN DE AUDITORÍA

Sistemas y Seguridad de la Información

2. OBJETO

Verificar la eficacia, eficiencia y efectividad del Sistema Integrado de Gestión (MECI_SGC), a través del Proceso de Sistemas y Seguridad de la Información de acuerdo a la ISO 9001:2008, ISO14001: 2004, OHSAS 18001: 2007 y MECI 2014 y demás normatividad aplicable a cada uno de los procedimientos del proceso.

3. ALCANCE DE LA AUDITORÍA

Cubre la implementación, desarrollo, evaluación y sostenibilidad del Proceso de Sistemas y seguridad de la Información a través de los procedimientos que tiene establecido el Proceso.

4. CRITERIOS AUDITORÍA

- Decreto 416 de 2016. Establece los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a través del posicionamiento de los líderes de áreas TI.
- Directiva presidencia 02 de 2015. Buenas prácticas para el ahorro de energía y agua
- Ley 1712 de 2014. Ley de Transparencia.
- Decreto 2573 de 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 103 de 2015. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Resolución 1315 de 2012
- Directiva Presidencial 04 de 2012. Eficiencia administrativa y lineamientos de la política cero papel en la administración pública.
- Resolución 564 de 2011 Por la cual se crea el Comité Técnico de Seguridad de la Información - CTSI - del Concejo de Bogotá D.C. y se definen sus funciones. Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- Decreto 235 de 2010. Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
- Resolución 305 de 2008. Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
- Acuerdo 279 de 2007.Por el cual se dictan los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
- Directiva 005 de 2005. Políticas Generales de Tecnologías de Información y

Comunicaciones aplicables a las entidades del Distrito Capital.

- Acuerdo 057 de 2002. Por el cual se dictan disposiciones generales para la implementación del sistema distrital de información -SDI-, se organiza la comisión distrital de sistemas, y se dictan otras disposiciones.
- Directiva Presidencial 02 de 2002. Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).
- Manual de Procesos y Procedimientos de la Corporación.
- Manual de funciones y competencias laborales del Concejo.
- Mapa de Riesgos.
- Caracterización.
- Indicadores.
- Planes de Contingencia
- Planes Estratégicos de la Información.
- ISO 9001:2008
- ISO 14001:2004
- OSHAS 18001:2007
- MECI 2014
- NTCGP 1000:2009

Y demás normatividad que sea aplicable al proceso.

5. RESPONSABLE /PROCESO/ DEPENDENCIA

Gloria Verónica Zambrano / Directora Administrativa

6. EQUIPO AUDITOR

Ingrid Beatriz Acosta Velásquez

7. AUDITADOS

Carlos Alberto Muñoz

8. METODOLOGÍA

Se realizó reunión de apertura, con todos los funcionarios de Sistemas y seguridad de la información, donde se dio a conocer el plan de auditoria, la cual señalaba las fechas de la auditoria, los auditores y los auditados. La auditoría se realizó mediante entrevista donde se levantó acta de reunión apoyada con la revisión de documentos.

9. PERÍODO DE EJECUCIÓN DE LA AUDITORÍA

Del 25 de Abril al 26 de Mayo de 2017

10. FORTALEZAS

- Es importante resaltar la buena disposición que tuvieron los funcionarios al atender la auditoria, así como la aceptación de las recomendaciones dadas sugeridas por el auditor con el propósito garantizar la mejora continua dentro del procedimiento, de igual manera se observó un equipo de trabajo comprometido al cumplimiento de los objetivos del proceso.

11. NO CONFORMIDADES POTENCIALES

**11.1** Aunque el proceso de Sistemas y Seguridad de la Información tiene establecida una caracterización la cual fue actualizada en la vigencia 2016, en revisión de la misma se observó que esta debe de ser ajustada nuevamente y que se incluyan todas las actividades propias de la gestión del proceso, a continuación se sugieren algunas actividades a tener en cuenta, tales como:

| PROVEEDOR | ENTRADA | ACTIVIDAD PHVA | SALIDAS | CLIENTES |
|---|---|---|---|---|
| Comisión Distrital de Sistemas MINTIC | Normatividad, lineamientos estrategias de gobierno en línea. | (Planear) Formular y/o actualizar el Plan Estratégico de Sistemas de Información | Plan Estratégico de Sistemas de Información | Comisión Distrital de Sistemas<br><br>Proceso de Sistemas |
| Proveedor de servicios de Internet, empresa encargada de mantenimiento y renovación firewall | Conectividad, redes, software especializado (firewall, antivirus) | (Planear) Administración de redes y servidores | Servicio de Internet para usuarios, seguridad de la información y conexión a dispositivos | Todos los procesos |
| Dirección Administrativa (todos los procesos) | A través de la Dirección administrativa se recibe todas las PQRS tales como: creación, modificación y/o retiro de usuarios | (Hacer) Administración de cuentas de usuarios, actualización de usuarios en el directorio activo, (correos, equipos y aplicativos), | Recibo a satisfacción por parte de los usuarios, registro en la bitácora de la solicitud de usuario o perfiles creados para acceso a equipos | Todos los procesos<br><br>Proceso de Sistemas |
| Proceso Evaluación Independiente | Informe Preliminar e Informe Definitivo | (Actuar) Proyección de objeciones, toma de acciones correctivas y/o preventivas | Plan de Mejoramiento | Proceso Evaluación Independiente |

Estos ajustes tienen el propósito de que sean identificados todos los factores intervinientes en la gestión propia de los procedimientos adscritos al proceso de sistemas y seguridad de la información, debe realizarse cuidadosamente, de manera que ésta caracterización sea coherente y consistente. Por lo tanto se debe mantener un "hilo conductor" a través de toda la caracterización. Lo anterior podría generar un posible incumplimiento de la NTCGP 1000:2009 4.1 Requisitos Generales, MECI 2014 Componente Direccionamiento Estratégico, Elemento Modelo de Operación por Procesos.

**11.2** Revisados los procedimientos del proceso de Sistemas y Seguridad de la Información, se observó que si bien los procedimientos fueron actualizados en su gran mayoría en la vigencia 2016 es necesario revisarlos nuevamente y ajustarlos de acuerdo a la gestión propia del mismo, en el entendido que los procedimientos son utilizados para delinear los pasos que deben ser seguidos por una dependencia e implementar la seguridad relacionada con dicho proceso, generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca cómo les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde

ellos se aplican. Para este proceso de Sistemas y Seguridad de la Información que tiene 12 procedimientos a su cargo, se hace necesario ajustar los responsables de la ejecución de las actividades, ajustar o modificar la redacción de algunas actividades, registrar en relación de empleos que intervienen los funcionarios que realmente ejecutan las actividades, asi mismo se sugiere realizar la eliminación de algunas actividades que por mejora continua o autoevaluación ya no se realizan, entre otros aspectos generales que se mencionan a continuación, discriminados por cada uno de los procedimientos adscritos al proceso, asi:

**Procedimiento Realización Copias de Seguridad Backup:**

Numeral 6: Descripción de Actividades

Numeral 6.1: En este numeral se establece que hay un equipo de infraestructura tecnológica que gestiona, monitorea, realiza medición, evaluación y ejecuta proyección de recursos para realizar las copias de seguridad, y según la relación de empleos hay 3 funcionarios: 2 profesionales y 1 auxiliar, lo que da a entender que todos los 3 realizan las mismas actividades de monitoreo, evaluación etc. se sugiere dejar claro quién debe realizar estas actividades, de acuerdo al manual de funciones y competencias del Concejo de Bogotá, toda vez que un auxiliar no debería realizar funciones de un profesional.

En el segundo párrafo de esta actividad se indica que una vez verificada la capacidad de los medios magnéticos existentes, se informa al Comité Directivo del Sistema Integrado de Gestión la necesidad de adquisición de medios y es este último seria quien gestiona la adquisición para la realización de copias de seguridad, de lo anterior se debe volver a redactar toda vez que el Comité Directivo SIG no gestiona la compra de medios magnéticos, el responsable directo de gestionar cualquier adquisición es el Director Financiero de la Entidad de acuerdo a unas fichas técnicas que el profesional especializado de Sistemas y seguridad de la información le envía de acuerdo a las necesidades que surgen para garantizar cumplir con el objeto del procedimiento.

Numeral 6.2 Activos de Información: indica que se realizara Backup a la información institucional misional de la corporación, se recomienda establecer la periodicidad de esta programación, el responsable o la referencia de dónde puedo encontrar esta frecuencia de realización de Backups.

En el segundo párrafo se sugiere eliminar él es responsabilidad de, e indicar tácitamente que los delegados de cada uno de los procesos de la entidad deben realizar clasificación de los activos de información digital que garantice el aseguramiento de la información sensible y critica.

En el tercer párrafo se hace necesario establecer quienes son los administradores de los servicios informáticos misionales y administrativos y redactar nuevamente el párrafo, toda vez que no es claro que si informan al administrador de la plataforma cual es el

procedimiento que se debe realizar, cada cuanto deben informar y en que formato.

Numeral 6.3 Programar copias de seguridad: se sugiere indicar en donde se realiza la programación y cada cuanto se realiza, asi como quien es el administrador de la plataforma.

En la parte de tareas de Backup de Exchange server, se recomienda eliminar el primer renglón, porque en la primera parte de la actividad se identificará quien es el responsable de la ejecución de los Backups.

Numeral 6.5 Realizar mantenimiento software: se hace necesario indicar cuál es el equipo e infraestructura, cuales son los profesionales que ejecutan esta actividad.

Numeral 6.6 Revisar información y verificar espacio en discos. Se sugiere registrar que esta actividad se realiza a diario.

Numeral 6.8: Rotación de medios: se recomienda indicar si los dos profesionales realizaran esta actividad y registrar que esta actividad se realiza semestralmente.

Numeral 9 Riesgos y Controles: se hace necesario eliminar el ver mapa de riesgos de corrupción de la corporación, toda vez que no están establecidos riesgos de corrupción para este procedimiento, o si se tiene pensado identificar riesgos de corrupción para estas actividades, se hace necesario actualizar el mapa de riesgos de corrupción.

**Procedimiento Atencion de Soporte Tecnológico:**

Numeral 5. Relación de empleos que intervienen en el procedimiento: se sugiere sacar al Director Administrativo de esta relación, toda vez que este cargo no tiene ninguna injerencia en estas actividades.

Numeral 6.1.4 Dar solución al caso reportado y documentar: en el segundo párrafo se menciona que el sistema de mesa de ayuda verifica la documentación de los casos atendidos por el equipo de soporte técnico. De lo anterior es necesario volver a redactar porque un sistema de mesa de ayuda no verifica nada, esta actividad es realizada por algún funcionario adscrito a la dependencia, además se hace necesario precisar en algún párrafo quienes conforman el equipo de soporte técnico.

Numeral 6.6 Informe y estadísticas: en el segundo párrafo de esta actividad se menciona que le sistema de mesa de ayuda entrega el diagnóstico de equipos de cómputo y periférico, de lo anterior se difiere toda vez que el sistema solo no realiza entregas de diagnósticos, por lo anterior es necesario volver a redactar el párrafo, de tal manera que quede claro que funcionario realiza el diagnóstico, ejecuta la entrega y a quien se la entrega, lo que sería insumo para el PETI.

Numeral 9: Riesgos y Controles: eliminar el ver mapa de riesgos de corrupción de la corporación, toda vez que no están establecidos riesgos de corrupción para este procedimiento, o si se tiene pensado identificar riesgos de corrupción para estas actividades, se hace necesario actualizar el mapa de riesgos de corrupción.

**Procedimiento Administración y actualización de la red y servidores:**

Numeral 6.1 Administración de IT: se sugiere eliminar el primer párrafo toda vez que a medida que se vayan describiendo las actividades se mencionan a los responsables de ejecutarlas, en el segundo párrafo de este numeral es preciso mencionar que el profesional especializado y el profesional universitario verifica diariamente el funcionamiento de la plataforma tecnológica, y se recomienda no mencionar el equipo de IT, a menos que se describa cuáles son los integrantes del equipo dentro de la actividad. El tercer párrafo menciona la responsabilidad de las credenciales de acceso a los activos son responsabilidad del equipo, este último párrafo se sugiere eliminarlo, en el entendido que a medida que se van describiendo las actividades se van indicando a los responsables.

Numeral 6.2 usuarios: se sugiere mencionar en el primer párrafo de este numeral a los 2 profesionales especializado y/o universitario, eliminando la denominación administrador del directorio activo, porque hace suponer que hay diferentes administradores para cada actividad específica.

Numeral 6.3 Monitoreo: en el primer párrafo se recomienda mencionar el profesional especializado y/o profesional universitario tal y como se describe en los demás párrafos siguientes, con el fin de que haya secuencia y para que no se preste a confusión, creyendo que el equipo de infraestructura tecnológica es diferente a los profesionales. En este mismo párrafo se sugiere relacionar el Ver Plan de contingencias, toda vez que en este último se encuentran descritas las diferentes actividades de mantenimiento preventivo que se realizan a diario. En el tercer párrafo de este numeral se menciona
Que los profesionales revisan a nivel de software "eventos" del sistema operativo periódicamente, se hace necesario establecer con qué frecuencia se realiza, a diario, mensual, semestral etc.

En el quinto párrafo de este numeral se recomienda colocar si el control de fallas se diligencia a través de una planilla, aplicativo, servidor y como controla los posible eventos que pueden llegar a ocasionar conflictos, en el sexto párrafo se sugiere mencionar al profesional especializado y/o universitario quien ejecuta acción preventiva y/o correctiva, asi como en el último párrafo de este numeral colocar a los profesionales intervinientes y establecer la periodicidad de ejecución de la actividad por medio de cuales sistemas operativos.

Numeral 6.4 Administración de cambios: se sugiere que en esta actividad se describa claramente donde se realiza la planeación que refiere este párrafo, cada cuanto se

realiza, como se realiza y quien es el responsable de ejecutarla.

Numeral 6.5 Control de seguridad y seguimiento: Numeral 6.6 realizar registro: mencionar al profesional especializado y/o profesional universitario y periodicidad en que se realiza la actividad.

Numeral 8. Políticas de operación. Colocar N/A toda vez que revisando las políticas operación no se tuene ninguna que tenga relación con este procedimiento.

Numeral 9. riesgos y Controles: eliminar el ver mapa de riesgos de corrupción de la corporación, toda vez que no están establecidos riesgos de corrupción para este procedimiento, o si se tiene pensado identificar riesgos de corrupción para estas actividades, se hace necesario actualizar el mapa de riesgos de corrupción.

**Procedimiento de Etiquetado y Clasificación:**

En este procedimiento se debe indicar la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad. Adicionalmente se debe explicar cómo se hace una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros lugares de manera segura.

Numeral 5. Relación de empleos que intervienen en el procedimiento: menciona que todos los servidores públicos del Concejo de Bogotá son los directamente responsables de gestionar, clasificar, etiquetar y proteger la información, de lo anterior se difiere toda vez que se sugiere asignar por proceso un responsable que realice estas actividades.

Numeral 6.1 Identificar la información y el medio de almacenamiento: se recomienda redactar nuevamente e identificar quien son los responsables directos de realizar esta actividad, asi como hace falta incluir en este párrafo como se debe almacenar según el tipo medio y en donde se almacena.

Numeral 6.2 Clasificar la información: es importante mencionar quien y cada cuanto se debe realizar esta actividad según lo que establece la guía de clasificación y etiquetado.

Numeral 6.5 Distribuir la información: en primer lugar e4s importante que se mencione cual es la información que se va a distribuir, como se realiza y a través de qué medios o canales, cada cuanto lo ejecuto y quién?

Numeral 8. Políticas de operación. Colocar N/A toda vez que revisando las políticas operación no se tiene ninguna que tenga relación con este procedimiento.

Numeral 9. riesgos y Controles: eliminar el ver mapa de riesgos de corrupción de la

corporación, toda vez que no están establecidos riesgos de corrupción para este procedimiento, o si se tiene pensado identificar riesgos de corrupción para estas actividades, se hace necesario actualizar el mapa de riesgos de corrupción.

**Procedimiento gestión de incidentes de seguridad de la información:**

Este procedimiento debe indicar como responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o Confidencialidad. Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los Planes de Continuidad dependiendo de la criticidad de la información.

Numeral 4. Aplicativos, instructivos, documentos y formatos utilizados: Hace falta colocar el aplicativo de mesa de ayuda.

Numeral 6.1 Planear actividades de capacitación: en este numeral se debe describir que el oficial de Seguridad de la Información planea actividades para prevenir incidentes de seguridad de la información, por otra parte aquí mismo se relaciona un listado donde se describen actividades que realiza el oficial de seguridad que se sugiere se retiren toda vez que no son desarrolladas tales como: auditorias periódicas y realizar esquemas de seguridad de fortalecimiento de los equipos de cómputo y colocar las demás que si realiza.

Numeral 6.2 Reportar eventos de seguridad: se sugiere colocar en esta actividad quienes y como se deben reportar los incidentes de seguridad de la información, a través de qué medios se realiza y cuál es el mecanismo utilizado para que los visitantes informen el evento detectado, se les entrega volantes informativos?, se les brinda algún acompañamiento y si los visitantes no tienen injerencia en estos eventos se recomienda no incluirlos en la relación de empleos que intervienen en el procedimiento, en este numeral también se hace necesario colocar si se les realiza o realizara sensibilización a los funcionarios en cuanto a cómo detectar un incidente, cuales son incidentes y cuales son asuntos de fácil solución.

Numeral 6.3 Evaluar el reporte del evento: se sugiere comenzar la redacción indicando que el oficial de seguridad de la información será el encargado de evaluar el evento y determinar si es incidente o una falsa alarma. Sin embargo se hace necesario realizar capacitación a los funcionarios en cuanto a determinar la diferencia entere incidente y falsa alarma y como tratar cada uno de los dos aspectos. Asi mismo se recomienda describir como se evalúa y que debe reportar resultado de esa evaluación.

Para las demás actividades descritas en el procedimiento se recomienda revisar los siguientes aspectos tales como: redacción, responsables, periodicidad y utilización de las

herramientas de gestión, verificar si se han identificado políticas de operación, riesgos de gestión y riesgos de corrupción para este procedimiento.

**Procedimiento Acceso físico:**

En este procedimiento se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas. (Estos procedimientos pueden tener la participación del área de seguridad y vigilancia de la entidad).

Numeral 6.2 permanencia en las oficinas de visitantes: por redacción de la denominación del numeral se debe colocar permanencia de los visitantes en las diferentes oficinas del Concejo de Bogotá: se sugiere describir en este numeral que sucede en caso que la persona que autorizo la entrada no realiza el debido acompañamiento del visitante y esta persona hurto o tuvo acceso a algún equipo de cómputo, o si sustrajo documentación confidencial. Cuáles son los controles que se tienen y si el personal de seguridad realiza rondas de inspección, estas con qué frecuencia se realizan?

Numeral 8 Políticas de operación: revisar si dentro del manual de políticas de operación de proceso de sistemas y seguridad de la información, se encuentra alguna política que establezca algún lineamiento para el ingreso y transito seguro entro de las oficinas del Concejo de Bogotá.

Numeral 9. riesgos y Controles: eliminar el ver mapa de riesgos de corrupción de la corporación, toda vez que no están establecidos riesgos de corrupción para este procedimiento, o si se tiene pensado identificar riesgos de corrupción para estas actividades, se hace necesario actualizar el mapa de riesgos de corrupción.

**Procedimiento Acceso lógico:**

En este procedimiento la entidad debe indicar como gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques, validando los datos completos para ingreso a los sistemas, empleando métodos para cifrar la información de acceso a través de la red entre otros.

Numeral 6.Descripcion de actividades:

Numeral 6.1. Solicitud de acceso a los sistemas de información: en este numeral se sugiere indicar que los diferentes procesos de la Entidad envían a la Dirección Administrativa memorando solicitando asignación de usuarios, equipos y privilegios, y esta última a través de memorando solicita al procesos de sistemas y seguridad de la

información la información requerida acorde con la función que cumplirá el funcionario.

Numeral 6.2: Asignación de acceso a los sistemas de información: se recomienda indicar cuál de los profesionales realizará esta actividad o si los dos tanto el especializado como el universitario dependiendo la carga laboral realizaran esta actividad.

Numeral 6.5 Solicitud de retiro de acceso a los sistemas de información: se sugiere en este numeral redactar que por previa solicitud de las diferentes dependencias y/o procesos de la entidad a través de memorando a la Dirección Administrativa, esta última emitirá un memorando de solicitud de retiro o cancelación de acceso y/o privilegios, teniendo en cuenta el cambio de rol del funcionario o renuncia del mismo a la Entidad.

Numeral 6.6. Retiro de acceso y privilegios a los sistemas de información: se recomienda establecer cuál de los dos profesionales ejecutara la actividad o si los dos, teniendo en cuanta su caga laboral.

Numeral 6.7. Revisión lista de acceso a los sistemas de información: en este numeral se menciona que se revisara periódicamente la lista de acceso a los sistemas de información, de lo anterior se hace necesario establecer la periodicidad, si es mensual, trimestral.. etc.

Numeral 8 y 9. En estos dos numerales se hace necesario establecer si se encuentran establecidos políticas de operación, riesgos de gestión y/o riesgos de corrupción asociados a este procedimiento.

**Procedimiento Administración equipos de cómputo:**

Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la Entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc... De igual manera en este procedimiento debe especificarse como los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc....), por otra parte se sugiere tener en cuenta que en este procedimiento se debe especificar como se ejecutan los mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores, se debe especificar el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.

Numeral 6.2 Asignación de equipos de cómputo por demanda: se recomienda indicar cual

funcionario de la relación de empleos realiza la asignación de equipos de cómputo a las diferentes áreas de la entidad.

Numeral 6.3 recibir solicitud de equipos: en este numeral se menciona que el Director administrativo o Director financiero, autoriza la asignación de los elementos tecnológicos o equipos de cómputo, de lo anterior se observa que el Director Financiero no aparece relacionado en el registro de personal interviniente en el procedimiento. Por lo cual se hace necesario establecer claramente la responsabilidad de ejecución de esta actividad y registrarlo en el Numeral 5.

Numeral 6.4 Entrega de equipos de cómputo: se recomienda indicar cual funcionario de la relación de empleos hace entrega del equipo de cómputo a los funcionarios. Si son varios los que realizan esta gestión, indicar que cargos. Al igual cuales funcionarios diligencian documentos para la asignación de los elementos de tecnología, asi como indicar quien son los integrantes del equipo de soporte técnico.

Numeral 8 y 9. En estos dos numerales se hace necesario establecer si se encuentran establecidos políticas de operación, riesgos de gestión y/o riesgos de corrupción asociados a este procedimiento.

**Procedimiento Gestión de la Capacidad:**

En este procedimiento se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc.

Numeral 5. Relación de empleos que intervienen en el procedimiento: se recomienda sacar de la relación de empleos que intervienen en el procedimiento al Director Administrativo, toda vez que en ninguna actividad descrita aparece la gestión del mencionado director.

Numeral 6.1 Realizar diagnóstico de la infraestructura tecnológica: en este numeral es preciso colocar cuál de los dos profesionales ejecutara la actividad, o si los dos la realizan mencionar a los dos profesionales, asi mismo en el segundo y tercer párrafo indicar la frecuencia en que se ejecuta la actividad y si el equipo de soporte técnico es el mismo equipo de infraestructura tecnológica, en el entendido que no es claro si son los dos profesionales que conforman diferentes equipos tales como equipó de soporte técnico y equipo de infraestructura. Por otra parte en el tercer párrafo es necesario redactar nuevamente toda vez que menciona que de definen unos indicadores de capacidad de los recursos, lo cuales no se han formulado ni medido.

Numeral 6.2 Monitorear la Capacidad: es necesario se vuelva a redactar este numeral indicando quienes o quien es el responsable de realizar este monitoreo, con que periodicidad se ejecuta y definir claramente cuáles son los parámetros o herramientas que se utilizan en el desarrollo del monitoreo.

Numeral 6.3 Identificar necesidades de capacidad: se recomienda que se describa apropiadamente la realización de esta actividad, toda vez que como en el párrafo anterior se mencionan evaluación de rangos aceptables y críticos de los indicadores, de los cuales no se tiene referencia.

Numeral 6.4 Informe de necesidades: en este numeral se menciona que el Comité Directivo del SIG, gestiona los recursos necesarios para suplir las necesidades de IT de la Corporación, lo que no es cierto, toda vez que el Comité No es responsable directo de la consecución de los recursos de la Entidad.

Numeral 8 y 9. En estos dos numerales se hace necesario establecer si se encuentran establecidos políticas de operación, riesgos de gestión y/o riesgos de corrupción asociados a este procedimiento.

**Procedimiento plan de necesidades de contratación y seguimiento a los contratos de tecnología:**

Numeral 6.1 Revisar estructura de red, servidores y reportes técnicos: se sugiere establecer que la revisión del componente hardware, software y la administración de los servidores tanto de la red como del licenciamiento se realiza a diario.

Numeral 6.2 Relacionar las necesidades de los funcionarios: se recomienda establecer en donde se realiza esta actividad o mediante que herramienta o documento queda registrada la relación de necesidades y/o daños.

Numeral 6.3 Elaborar Solicitud de contratación vigencias futuras: se debe retirar esta actividad oda vez que no es realizada por el proceso de sistemas y seguridad de la información.

Numeral 6.10 verificar legalización de contrato y acta de inicio: es importante mencionar en esta actividad que las carpetas de estos contratos de sistemas y seguridad de la información reposan en el archivo de fondo cuenta del Concejo de Bogotá, y son ellos que realizan la debida conservación, disposición, Organización de la información.

Numeral 8 y 9. En estos dos numerales se hace necesario establecer si se encuentran establecidos políticas de operación, riesgos de gestión y/o riesgos de corrupción asociados a este procedimiento.

Lo anterior podría generar un posible incumplimiento de la norma NTCGP 1000:2009 4.1 Requisitos Generales Literal b) 4.2.3 Control de documentos 4.2.4 Control de registros, ISO 9000:2008 numeral 4.2.3 y 4.2.4 MECI 2014 Eje Transversal, Información y Comunicación.

**11.3** Si bien se tienen aprobadas las políticas de operación del proceso Sistemas y Seguridad de la Información, se observó que es necesario realizar un nuevo ajuste de las políticas, en cuanto a redacción y responsabilidad de ejecución, a continuación se describen los aspectos a tener en cuenta en la revisión:

Numeral 4.2 en esta política se menciona que la Dirección Administrativa deberá mantener copias de seguridad, en medio magnéticos diferentes a los discos duros, para restauración de la información. De lo anterior se recomienda no argumentar que la Dirección Administrativa mantendrá copias de seguridad, toda vez que el proceso que tiene el lugar de almacenamiento de estas copias es Sistemas de Seguridad de la Información en sus cintotecas.

Numeral 4.4 en esta política se evidencia un posible incumplimiento toda vez que se indica que le Concejo de Bogotá implementara un Sistema de gestión de Seguridad de la información, basado en una aproximación de los riesgos, mejorar, operar, monitorizar, revisar y mantener la seguridad de la información, con respecto a este Sistema se puede observar que si bien se ha adelantado mucha información documental aún hace falta actualizar otra conforme a la normatividad que lo regula, asi como realizar otras actividades o acciones propias que garanticen que la entidad logre la certificación para posterior implementación y mejora.

Numeral 4.6 se hace importante en esta política describir cuales recursos son necesarios para garantizar el correcto desarrollo y cuáles fueron los lineamientos dados por la alta dirección.

Numeral 4.7 en esta política se describe que la alta dirección establecerá los criterios de evaluación del riesgo asi como que la alta dirección desarrollara, implantar y mantendrá actualizado un plan de continuidad. De lo anterior se difiere toda vez que la alta dirección realiza revisión por la dirección y brinda lineamientos claros de trabajo mas no desarrolla, implementa y mucho menos actualiza los planes de continuidad de la entidad, por tal motivo se requiere volver a redactar la política.

Numeral 4.12 se menciona que el Concejo de Bogotá supervisa a través de circuito cerrado de televisión el comportamiento de las personas al interior de sus sedes, de lo anterior se sugiere cambiar el concejo de Bogotá por vigilancia, toda vez que es este último quien realiza la actividad.Lo anterior podría generar un posible incumplimiento de la Norma NTCGP 1000:2009 4.2 Gestión Documental 4.2.1 Generalidades literales a, b, c y d 5.2 Enfoque la cliente MECI 2014 Eje Transversal: Información y Comunicación, Modulo: Planeación y Gestión Componente: Direccionamiento Estratégico Elemento:

Políticas de Operación.

No Conformidad Compartida con la oficina asesora de planeación:

**11.4** De acuerdo al plan de acción aprobado mediante resolución 333 del 16 de Mayo de 2017, se realizó una revisión de las actividades que están bajo responsabilidad del proceso de sistemas y seguridad de la información que se encuentra publicado en la red interna de la Entidad, a través del link de Planeación y se identificaron los siguientes aspectos que podrían llegar a presentar incumplimiento de la realización de las actividades allí descritas tales como:

| | | | |
|---|---|---|---|
| **12- Sistemas y Seguridad de la Información** | 26 | Proveer un servidor | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| | 27 | Proveer o actualizar licencias para el Servidor | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| | 28 | Proveer licenciamiento de Correo Electrónico | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| | 29 | Proveer un sistema de seguridad y protección de Amenazas de Red | Plataforma Tecnológica Actualizada Adquisición de Software |
| | 30 | Proveer 45 portátiles para el Concejo | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| | 31 | Proveer un software para monitoreo de Red y Servidores | Plataforma Tecnológica Actualizada Adquisición de Software |
| | 32 | Proveer el sistema de streaming de Audio y Video | Plataforma Tecnológica Actualizada Adquisición de Software |
| | 33 | Proveer un software para Diseño Grafico | Plataforma Tecnológica Actualizada Adquisición de Software |
| | 34 | Adición y prorroga al contrato 160304 de 2016, servicios técnicos que garanticen el correcto funcionamiento de la Libreria de Backups LTO 7 | Plataforma Tecnológica Actualizada Adquisición de Software |
| | 35 | Proveer un sistema de Red Inalámbrica. | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| | 36 | Adquirir soluciones tecnológicas Integrales para el Concejo de Bogotá. Realizar trámites para la adquisición del sistema de Voto Electrónico del Recinto de los Comuneros en materia de Sonido, y demás Tecnologías para la realización de las sesiones de los Honorables Concejales. | Recinto los Comuneros adecuado en materia de sonido y voto electrónico. Renovación del sistema de voto electrónico por obsolescencia tecnológica , el actual sistema cumplió su vida útil |

De acuerdo a las actividades anteriormente registradas en el cuadro, se encontraron las siguientes observaciones a tener en cuenta:

Actividades 26, 27, 28, 29, 30, 31, 32, 33, 34, 35 y 36. Proveer un servidor, Proveer o actualizar licencias para el Servidor, Proveer licenciamiento de Correo Electrónico, Proveer un sistema de seguridad y protección de Amenazas de Red, Proveer 45 portátiles para el Concejo, Proveer un software para monitoreo de Red y Servidores, Proveer el sistema de streaming de Audio y Video, Proveer un software para Diseño Gráfico, Adición y prorroga al contrato 160304 de 2016, servicios técnicos que garanticen el correcto funcionamiento de la Librería de Backups LTO 7, Proveer un sistema de Red Inalámbrica. Adquirir soluciones tecnológicas Integrales para el Concejo de Bogotá. Realizar trámites para la adquisición del sistema de Voto Electrónico del Recinto de los Comuneros en materia de Sonido, y demás Tecnologías para la realización de las sesiones de los Honorables Concejales.

Se observa que las anteriores actividades de proveer estos recursos no están en cabeza del proceso de sistemas de seguridad de la información, sino son responsabilidad directa de la Dirección financiera a través de fondo cuenta, por tanto la actividad debería establecerse o describirse como realizar el trámite de la solicitud mediante ficha técnica, según estudios IT del concejo de Bogotá. Lo anterior podría generar un incumplimiento del plan acción 2017, toda vez que como ha sucedido en vigencias anteriores, el proceso de sistemas realiza todos los tramites pero la consecución de los recursos no se realiza a tiempo o simplemente no se realiza la contratación y el cumplimiento de la actividad quedaría en cero 0% de ejecución. Por tanto se observa que la descripción de la actividad no corresponde a la gestión propia del proceso de sistemas y seguridad de la información.

De otra parte, a continuación se muestra el cuadro que corresponde a los indicadores de gestión del proceso de sistema y seguridad de la información que hace parte integral del plan de acción 2017.

| | | | |
|---|---|---|---|
| **12- Seguridad y Sistemas de Información** | 92 | Tramitar todas las solicitudes de contratación referente a la plataforma tecnológica del Concejo de Bogotá D.C. | Plataforma Tecnológica actualizada |
| | 93 | Planificar y Realizar las encuestas de satisfacción de los usuarios con relación al Proceso y Subsistema de Sistemas y Seguridad de la Información | Soporte en la Implementación del Subsistema de Gestión y Seguridad de la Información y Calidad de la Sostenibilidad del Procesos |
| | 94 | Dar soporte en software, aplicativos, hardware, a través de la mesa de ayuda del proceso de sistemas y seguridad de la información. | Soporte y Asistencia de Calidad tanto en software como hardware para mejorar la integridad de los servicios tecnológicos. |
| | 95 | Realizar las copias de seguridad de la información del Concejo de Bogotá D.C. | Medir la eficiencia y eficacia en la realización de copias de seguridad y de respaldo de la información, de conformidad con el Subsistema de Gestión y Seguridad de la Información |

Conforme a estas actividades se observa lo siguiente:
Actividad N. 92: Tramitar todas las solicitudes de contratación: esta labor estaría inmersa

en la gestión que se adelantaría en el primer cuadro con los trámites para garantizar la compra de los recursos tecnológicos, con respecto a las actividades 93, 94 y 95 no se realizan observaciones al respecto. Las anteriores observaciones se recomienda sean tenidas en cuenta para evitar un posible incumplimiento de la norma NTCGP 1000:2009 4.1 Requisitos Generales, literal c, d, e, f y g 5. Responsabilidad de la Dirección 5.1 compromiso de la Dirección 4.2 Gestión Documental 4.21 Generalidades c) d) 4.2.3 Control de Documentos, literal a y b 4.2.4 control de Registros, Numeral 5.4 Planificación, 5.6 revisión por la dirección. MECI 2014 Modulo de control de Planeación y Gestión, Componente Direccionamiento Estratégico, Elementos: Planes, Programas y proyectos.

**11.5** Si bien se ha venido trabajando para lograr la implementacion y Certificacion del Sistema de Seguridad de la informacion, en revision de los requisitos minimos que exige la noma 27001, aun faltan algunos procedimientos, documentos y acuerdos por realizar al interior de la entidad, a continuacion se encontraron los siguientes aspectos a tener en cuenta, lo que permitiria y garantizaria tener la certificacion en esta Norma, tales como:

A Considerar: *Literal de la Norma 27001: "NOTA 1 En esta norma, el término "procedimiento documentado" significa que el procedimiento está establecido, documentado, implementado y mantenido."*

*A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*
*A.6.1 Organización interna*

A.6.1.1 Compromiso de la dirección con la seguridad de la información: La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.

Observación Control Interno: Con respecto a este tema no se evidencia el compromiso de la dirección con la seguridad de la información toda vez que desde la vigencia 2016 se solcito la contratación para mantenimiento, mejora continua y certificación del Sistema de gestión de Seguridad de la Información bajo el estándar NTC-ISO /IEC- 27001:2013, y esta se reiteró a través de memorando IE9092 del 13-06-2016, y una vez revisado el plan de Anual de adquisiciones se observa que no quedaron apropiados los recursos para esta contratación.

*A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*
*A.6.1.5 Acuerdos sobre confidencialidad*

Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.

Observación Controlo Interno: Con respecto a este tema aún no se evidencia que se

hayan realizado los acuerdos de confidencialidad con los diferentes procesos de la entidad, si bien se ha llevado este tema ante el Comité Directivo del SIG y ante la Dirección Jurídica para que revise los acuerdos y a la fecha de la auditoria aún no se han pronunciado sobre este tema.

*A.7 GESTIÓN DE ACTIVOS*
*A.7.1 Responsabilidad por los activos*
*A.7.1.1 Inventario de activos Control*

Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.

Observación Control Interno: El inventario de activos se encuentra relacionado sin embargo es necesario realizar actualización con los nuevos equipos de cómputo que ingresaron a la entidad y demás activos que durante esta vigencia han ingresado a la entidad, de este punto se hace importante mencionar que los equipos de cómputo fueron solicitados hace un año, llegaron al almacén de Secretaria de Hacienda hace 4 meses y hasta finales del mes de Mayo de 2017, fueron entregados al Concejo de Bogotá, como es de conocimiento los equipos de tecnología presentan una rápida desactualización y las industrias del hardware y de software se mantienen en constante evolución tecnológica para conseguir mayores capacidades físicas de trabajo de las computadoras, este fenómeno no fue tenido en cuenta por la Secretaria de Hacienda y en actualmente el Concejo de Bogotá ya tiene equipos nuevos desactualizados.

A.7.2 Clasificación de la información
A.7.2.2 Etiquetado y manejo de información
Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización,

Observación Control Interno: si bien se tienen establecidos, documentados y aprobados los procedimientos de etiquetado y clasificación de la información, estos deben actualizarse como se mencionó anteriormente en la no conformidad potencial de procedimientos.

A.10.2 Gestión de la prestación del servicio por terceras partes
Objetivo: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.
A.10.2.1 Prestación del servicio Control

Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de Prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.

Observación Control Interno: No se tienen los acuerdos de prestación de servicios por terceras partes.

A.10.2.3 Gestión de los cambios en los servicios por terceras partes

Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.

Observación Control Interno: No se les ha realizado reevaluación a los riesgos establecidos.

*A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES*
*A.10.4 Protección contra códigos maliciosos y móviles*
*A.10.4.1 Controles contra códigos maliciosos.*

Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.

Observación Control Interno: En este punto se observa que no se han definido procedimientos documentados para la concientización de usuarios contra códigos maliciosos y si se va a establecer este procedimiento es necesario tener en cuenta lo siguiente:

La entidad debe indicar por medio de este procedimiento como realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo

*A.10.7 Manejo de los medios*
*Objetivo: evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.*
*A.10.7.1 Gestión de los medios removibles*

Se deben establecer procedimientos para la gestión de los medios removibles

Observación Control Interno: Frente a este aspecto se observa que actualmente el Concejo de Bogotá no tiene un procedimiento para la gestión de medios removibles.

*A.10.7.2 Eliminación de los medios.*

Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin Riesgo, utilizando los procedimientos formales.

Observación Control Interno: Igualmente se debe establecer procedimientos para la eliminación de los medios.

*A.10.8 Intercambio de la información*
*Objetivo: mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.*
*A.10.8.1 Políticas y procedimientos para el intercambio de información*

Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la Información mediante el uso de todo tipo de servicios de comunicación.

Observación Control Interno: Se observa que no se tiene procedimiento establecido para el intercambio de la información y si se va a establecer un procedimiento de intercambio de información se considera tener en cuenta lo siguiente:

En este procedimiento la entidad deberá indicar como realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.

Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

*A.10.8.2 Acuerdos para el intercambio*

Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.

Observación Control Interno: Frente a este numeral se observa que no se tiene establecidos los acuerdos para el intercambio de la información.

*A.10.10.2 Monitoreo del uso del sistema*

Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información y los resultados de las actividades de monitoreo se deben revisar con regularidad

Observación Control Interno: Se observa que actualmente no se tiene procedimiento para el monitoreo de uso de los servicios de procesamientos de la información.

*A.11 CONTROL DE ACCESO*
*A.11.2.1 Registro de usuarios.*

Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

Observación Control Interno: No se tiene un procedimiento establecido para el registro y cancelación de usuarios.

*A.11.2.4 Revisión de los derechos de acceso de los usuarios.*

La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de Acceso de los usuarios.

Observación Control Interno: No se tiene un procedimiento de revisión periódica de los derechos de acceso a usuarios.

*A.11.5.1 Procedimientos de ingreso seguro*

El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de Inicio seguro.

Observación Control Interno: No se tiene procedimiento de registro de inicio seguro.

*A.11.7.2 Trabajo remoto.*

Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Observación Control Interno: Si bien se tienen establecidas unas políticas establecidas para el teletrabajo, no se tiene un procedimiento para la realización de las actividades de trabajo remoto.

*A.13.1.2 Reporte sobre las debilidades de la seguridad*

Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y Servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Observación Control Interno: No se observa como se ha sensibilizado a los todos los

funcionarios de la entidad para que reporten las debilidades de la seguridad y cuáles serían las posibles debilidades, y como se reportan estas debilidades.

**A**.*14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO*

*A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio*

Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

A.*14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.*

Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

*A.14.1.2 continuidad del negocio y evaluación de riesgos*

Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio Junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

*A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información*

Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.

*A.14.1.4 Estructura para la planificación de la continuidad del negocio*

Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento

*A.14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio*

Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Observación Control Interno: La entidad actualmente cuenta con plan de contingencia pero no tiene establecido un plan de continuidad que establece la norma, toda vez que el

plan de contingencia podría estar incluido dentro del plan de continuidad, ya que este último incluye los controles a evitar que los riesgos se materialicen y el de contingencias ya establece correctivos una vez se han materializado asi mismo si se va a establecer un procedimiento es importante que tengan en cuenta lo siguiente:

En este procedimiento la entidad debe indicar la manera en que la entidad garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico. El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.

*A.15 CUMPLIMIENTO*

*A.15.1 Cumplimiento de los requisitos legales*

Objetivo*:* evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

A.15.1.1 Identificación de la legislación aplicable.

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y Mantener actualizados para cada sistema de información y para la organización.

Observación Control Interno: Es necesario mantener actualizado el Normograma de la Entidad, toda vez que hace alta incluir normas.

*A.15.1.2 Derechos de propiedad intelectual (DPI).*

Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Observación Control Interno: Tener en cuenta este numeral en caso de patentar un software para establecer el procedimiento respectivo.

OTROS ASPECTOS A CONSIDERAR:

A continuación se describen algunos aspectos a tener en cuenta, si se van a establecer y/o elaborar en el Concejo de Bogotá los siguientes procedimientos:

Procedimiento de Capacitación y Sensibilización del Personal:

Indica la metodología empleada por la entidad para realizar la capacitación y sensibilización del personal en temas de seguridad de la Información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones etc...

Procedimiento de Gestión de Usuarios y Contraseñas:
En este procedimiento, la entidad deberá indicar como realiza la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas.
Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

Lo anterior para evitar un posible incumplimiento de la norma NTCGP 1000:2009 4.1 Requisitos Generales, 5. Responsabilidad de la Dirección 5.1 compromiso de la Dirección 4.2 Gestión Documental 4.21 Generalidades c) d) 4.2.3 Control de Documentos, literal a y b 4.2.4 control de Registros, Numeral 5.4 Planificación, 5.6 revisión por la dirección. MECI 2014 Modulo de control de Planeación y Gestión, Componente Direccionamiento Estratégico.

***11.6*** Teniendo en cuenta la Resolución 934 de 2016 Artículo Séptimo establece que el oficial de seguridad de la información debe reportar a la Dirección Administrativa, oficina Asesora de planeación y al Comité se Seguridad de la información, pero no establece claramente que debe reportar el oficial, cual documento, en que formato y cada cuánto?

Por otra parte se hace necesario delegar un funcionario de la entidad que ocupe este cargo en el evento de contingencia que no se realice la contratación a tiempo del oficial de seguridad, este funcionario de planta ejercerá las funciones establecidas en la Resolución y dará continuidad y cumplimiento al desarrollo de las actividades descritas. De no cumplirse lo anterior durante la vigencia se podría incurrir en un posible incumplimiento de la Resolución 934 de 2016 Articulo 5. La norma NTCGP 1000:2009 4.1 Requisitos Generales, 5. Responsabilidad de la Dirección 5.1 compromiso de la Dirección 4.2 Gestión Documental 4.21 Generalidades c) d) 4.2.3 Control de Documentos, literal a y b 4.2.4 control de Registros

12. NO CONFORMIDADES REALES

**12.1** Incumplimiento de la Resolución 305 de 2008, Norma NTCGP 1000:2009 Gestión documental .2.3 Control de Documentos 4.2.4 control de Registros y 4.2.3 Documentos; MECI 1000:2014 1.2 Direccionamiento estratégico. Se evidencio que según lo descrito en los siguientes Artículos, el proceso de sistemas y seguridad de la información debe realizar las actividades allí descritas y a la fecha no se han ejecutado, tales como:

Capitulo Primero

**Artículo 18.** Planes de Contingencia, Parágrafo: el plan de contingencias que se adopte debe ser formulado conforme a una metodología específica para tal fin, contemplar todos los tipos de riesgo posibles para la entidad, establecer plan de manejo del riesgo y los planes de acción específicos en cada caso, ser avalado por la alta dirección, socializado en todos los niveles de la organización estableciendo las responsabilidades correspondientes y revisado periódicamente con el "planes estratégico de sistemas de información" y con cambios en las condiciones operativas de la entidad.

Conforme a los controles para cada dominio: la norma establece que se debe evaluar el impacto de los diferentes procesos en la entidad y realizar planes de mitigación y continuidad para aquellos que resulten críticos. Los planes de mitigación y continuidad deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente y deben permanecer articulados con los diferentes recursos tecnológicos y no tecnológicos existentes en toda la entidad.

De acuerdo a lo anterior se observa que la última fecha de presentación y actualización el plan de contingencias de la entidad se presentó en Abril de 2015, en el 2016 y en lo corrido de la vigencia 2017 no se ha actualizado el plan de contingencias y no se ha elaborado el plan de continuidad.

**Conceptos:**

**Plan de Contingencia** consiste en restar el impacto financiero que puede acusar un "incidente" inesperado en la compañía dentro del marco de los procedimientos habituales de la entidad, este plan trabaja para recuperar a la compañía de los imprevistos especiales que se puedan dar, y que por su causa **interrumpen el sistema de producción.**

Mientras que un **Plan de Continuidad** está enfocado a asegurar la continuidad del negocio, cuando de repente ocurre un incidente inesperado. Este plan lo que intenta es **no detener la productividad** de la entidad, e intentar que la situación que ha sucedido en ese momento nos afecte lo menos posible.

Muchas veces estos dos conceptos no se pueden desligar, un plan de contingencia puede estar dentro de un Plan de Continuidad, ya que lo que se busca con estas medidas es una rápida recuperación ante los desastres, para reanudar lo antes posible la cadena de producción.

Por otra parte en el numeral 9.21 Gestión de la continuidad del negocio. Establece que: el Concejo de Bogotá determinara los requisitos para la seguridad de la información y la

continuidad de la gestión de la seguridad de la información en situación crítica o de desastre

a) El Concejo de Bogotá revisara si la continuación de la seguridad de la información se ha incluido dentro del plan de continuidad de negocio.
b) El Concejo de Bogotá establecerá, documentara implementara y mantendrá procesos, procedimientos y controles que propendan por un nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
c) El Concejo de Bogotá, deberá verifica a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

De lo anterior se evidencia un incumplimiento toda vez que no se ha establecido el plan de continuidad del Concejo de Bogotá, de igual manera, el numeral 10 del manual de políticas de seguridad de la información, establece Sanciones: mencionando que estas políticas son obligatorias, por lo tanto deben ser cumplidas por todas las personas adscritas al concejo de Bogotá... y cualquier incumplimiento de las políticas y procedimientos de seguridad es considerado como falta disciplinaria por incumplimiento de las obligaciones y deberes del empleado que será sancionado en conformidad con lo previsto en la Ley y en el reglamento interno de trabajo.

**Artículo 50**. DIRECTRICES DE IMPLEMENTACION DE RACIONALIZACION DEL GASTO EN EL DC. Se destacan como directrices para la implementación de la racionalidad del gasto en materia de administración de bienes y recursos de infraestructura de tecnología de información y comunicaciones, los siguientes:

a) En materia de sistemas de apoyo administrativo, todas las entidades distritales en el momento de realizar una adquisición, deben evaluar como alternativa los sistemas de propiedad de otra entidad distrital que hayan sido homologados por la CDS. En particular se debe considerar como primera alternativa el Sistema de Información Hacendario.
b) Las compras en materia de tecnología informática que realicen las entidades deben ajustarse a los precios obtenidos en los convenios firmados por el Distrito con los proveedores de tecnología.
c) El Distrito establecerá los servicios que puedan ser prestados por entidades distritales y que no se contrataran con proveedores externos.
d) El costo de acceso a internet debe ser registrado por las entidades en el presupuesto de funcionamiento.
e) Los proyectos de implementación de sistemas de información deben garantizar una buena relación costo beneficio teniendo en cuenta aspectos como la oportunidad, la calidad, la integridad, la posibilidad de masificación y evolución tecnológica.

De lo anterior no se observa que la entidad haya tenido en cuenta los anteriores aspectos mencionados para garantizar una adecuada racionalización del gasto.

**Artículo 53**. Inventarios de los sistemas de información y de la infraestructura tecnológica: los jefes de las entidades, organismos y órganos de control del distrito capital deben actualizar la información correspondiente a los siguientes inventarios: "inventario de los sistemas de información administrativos y misionales" e "inventario de la infraestructura tecnológica relacionada con informática y comunicaciones". Aplicativos que se encuentran publicados para su actualización y diligenciamiento en la página web de la CDS.

De lo anterior no se encuentra la actualización de inventarios en la página www. bogota.gov.co/cds.

**Articulo 67** Políticas, Directrices y lineamientos para el uso del software libre en el Distrito Capital; Parágrafo 1: los jefes, o sus delegados, de las entidades, organismos y órganos de control del Distrito Capital....., deben presentar un informe trimestral al Presidente de la Comisión Distrital de Sistemas, los cuales se consolidaran y utilizaran para la presentación del informe semestral de que trata el artículo 2 del Acuerdo 279 de 2007.

**Articulo 68** Responsables de la promulgación, Difusión y aplicación de las políticas para la promoción y uso del software libre en el Distrito Capital: Todas las entidades, organismos y órganos de control del distrito capital deben enviar un informe el 1 de Junio y 1 de Diciembre de cada año, al presidente de la Comisión distrital de Sistemas, en el cual se reflejen los avances y resultados obtenidos respecto a la política de promoción y uso de software libre.

Con respecto a los artículos anteriores no se evidencia el envió de los informes trimestrales ni de los documentos con los avances y/o resultados obtenidos con la aplicabilidad de la política del Software libre del Concejo de Bogotá, asi mismo se observa que esta política se establecido en la Vigencia 2013 y en la presente vigencia se identificaron aspectos que se deben actualizar dentro del contenido de esta política, tales como:

a) El Concejo de Bogotá, establecerá medidas, estrategias y controles adecuados que garanticen la utilización del software libre asegurando una gestión segura de los procesos, primando la protección de la información.

De este literal no se observa las medidas, estrategias y controles que el concejo de Bogotá ha establecido para la utilización del software libre.

b) La alta dirección establecerá los criterios de evaluación del software libre de manera que todos aquellos escenarios que impliquen aplicabilidad sean evaluados para implantar y mantener actualizado acorde a las necesidades de la Corporación.

De este literal no se observa que la alta dirección haya establecido criterios de evaluación frente a esta política.

**12.2** Incumplimiento NTCGP 1000:2009, 6.2.2 Competencia, Formulación y toma de Conciencia, MECI 2014, Modulo Control de Planeación y Gestión, Componente Talento Humano, Elemento desarrollo del Talento Humano. Se observa que la estructura del proceso de sistemas y seguridad de la información se encuentra establecida asi: 2 (dos) Profesional Especializado 222-05 – funcionarios Ingeniero Carlos muñoz y William Ávila, 2 (dos) Profesional Universitario 219-03- Jeison Montaño y Linda Rosa Ocampo, 2 (dos)Técnicos Operativos – Jhon Neira y Raúl Rodríguez, 1 Secretario Ejecutivo - Orlando Vega y 3 (tres) Auxiliares Administrativos – Exse David Duarte, Alexandra Medrano y Deissy Yuranni Vega

Con respecto a lo anterior se evidencio que actualmente se tiene a una profesional universitaria 219-03 que se encuentra asignada al proceso de sistemas pero está ejerciendo funciones en el proceso de Nomina, Asi mismo se tiene a un Profesional Especializado al cual no se le han asignado funciones de acuerdo a su competencia para que apoye más técnicamente al proceso de sistemas por su experticia y conocimientos profesionales en este proceso, por otra parte se tiene un auxiliar administrativo realizando actividades de un profesional universitario, por lo anterior se considera que se deben tomar correctivos para que el proceso de sistemas y seguridad de la información de acuerdo a su estructura cuente con todo su personal que coadyuve a la cumplimiento de los objetivos, políticas y procedimientos del mismo.

**SEGUIMIENTO PLAN DE MEJROAMIENTO DE LA VIGENCIA 2016**

**12.3** Incumplimiento de la norma NTCGP 1000:2009 4.1 Requisitos Generales, 5. Responsabilidad de la Dirección 5.1 compromiso de la Dirección 4.2 Gestión Documental 4.21 Generalidades c) d) 4.2.3 Control de Documentos 4.2.4 control de Registros, 8.5.2 Acciones Correctivas 8.5.3 Acciones preventivas MECI 2014 2.3 Componente Planes de Mejoramiento, Incumplimiento al plan de mejoramiento de la vigencia 2016, se evidencio que las siguientes no conformidades no cumplieron con la realización de las acciones preventivas y/o correctivas

*NCP 11.5 Si bien se tiene establecido las guías de gestión de incidentes y de etiquetado y clasificación, no se evidencia utilización de estos dos documentos por parte del subsistema de sistemas y seguridad de la información. De igual forma no se evidencia acciones coordinadas con gestión documental para establecer la clasificación de la información de la entidad (publica, reservada, publica reservada). Lo anterior podría generar un incumplimiento a la Ley 1712 de 2014, ISO 9001:2008 5.4 Planificación; NTCGP 1000:2009 5.4 Planificación; MECI 2014 3. Eje transversal de comunicación.*

*La acción propuesta: el proceso de sistemas y seguridad de la información utilizara la guía de gestión de incidentes, etiquetado y clasificación. Asi mismo se solicitara a los*

*responsables de los procesos clasificar la información utilizada y/o generada, de igual manera el oficial de seguridad realizara la sensibilización a los procesos de cómo se debe clasificar la información.*

*Seguimiento: no se ha ejecutado la capacitación en temas de etiquetado y clasificación a los delegados y/o los jefes de los procesos por parte del oficial de seguridad de la información.* ***CONTINÚA ABIERTA.***

*NCR 12.2 Incumplimiento ISO 9001 8.5.1 Mejora; 8.5. 2 acción correctiva; 8.5.3 acción preventiva; NTCGP 1000:2009 8.5.1 Mejora; 8.5. 2 acción correctiva; 8.5.3 acción preventiva; MECI 2014 2.3 Planes de mejoramiento. Se evidenció que la empresa PASSWORD realizo auditoria a la Corporación para determinar el grado de implementación de seguridad de la información en noviembre de 2015, como resultado de esa auditoria se elaboró un plan de mejoramiento que a la fecha no se ha dado cumplimiento a las acciones implementadas por los responsables del Subsistema, ni se le ha hecho seguimiento*

*La acción propuesta: El oficial de seguridad de la información y el responsable del proceso de la seguridad de la información realizaran seguimiento y elaboraran el plan de mejoramiento establecido por la firma Password.*

*Seguimiento: no se evidencio cumplimiento de la acción propuesta.* ***CONTINÚA ABIERTA.***

**Evidenciada en sistemas y seguridad de la información y se traslada a la Dirección Financiera:**

**a)** Incumplimiento de la Resolución 305 de 2008, Norma NTCGP 1000:2009 Gestión documental .2.3 Control de Documentos 4.2.4 control de Registros y 4.2.3 Documentos; MECI 1000:2014 1.2 Direccionamiento estratégico. Se evidencio que según lo descrito en los siguientes Artículos, el proceso de sistemas y seguridad de la información debe realizar las actividades allí descritas y a la fecha no se han ejecutado, tales como: **Articulo 12 Parágrafo:** es responsabilidad de las entidades, organismos y órganos de control del Distrito capital gestionar los recursos tecnológicos y administrativos que permitan el manejo de los datos y la información, asi como controlar el uso de dichos recursos por parte de los funcionarios y los contratistas que los conforman.

Con base en lo anterior, se observa que la Dirección Administrativa desde la vigencia 2014 ha dejado de lado las reiteradas solicitudes de sistemas para la contratación en cuanto al fortalecimiento de recursos informáticos asi:

**Memorando Cordis IE15637 del 01-12-2014**, solicitud de contratación para la compra de herramientas para el mantenimiento preventivo y/o correctivo y reparación de los equipos de Cómputo PCS y Portátiles. Entre los que se encuentran: Destornilladores de precisión,

Cautín, crema para soldar, estaño, desolador de succión o chupón, juego de pinzas, Alicates, Llaves Bristol, Pela Cable ajustable, Multímetro, Ponchadora de Rj45, Mapeador de Red y probador de cables UPT, Disco duro Extraíble, Caja Conversara IDE/SATA a USB, Pasta térmica para procesadores, Manillas antiestática, linterna recargable LED, Pegamento Instantáneo, Martillo, Brocha, Cinta METRICA, Mazo de Goma, Aceite lubricante en spray, Espuma limpiadora de pantallas y teclados, limpiador de contactos aerosol, lasta de aire comprimido, Kit limpiador para lentes de unidades de Cd/DVD, 4 rollos de cinta aislante, tapabocas industriales, bisturí grande y pequeño, alcohol isopropilico, copos de algodón, bayetilla blanca.

**Memorando Cordis IE1198 del 12-02-2015**, solicitud reiterando compra de las herramientas necesarias para el cumplimiento de las funciones de los funcionarios del proceso de sistemas y seguridad de la información.

**Memorando Cordis IE5875 del 19-04-2016,** solicitud para la adquisición de un sistema de detección de incendios para el centro de cableado del edificio del Concejo de Bogotá.

**Memorando Cordis IE9092 del 13-06-2016**, respuesta solicitudes, se informa que no quedaron apropiados recursos para las siguientes solicitudes: compra de herramientas, mantenimiento, mejora y certificación del SGSI ISO 27001:2013.

**Memorando Cordis IE1983 del 09-02-2017**, envió ficha técnica para la adquisición del sistema de detección de incendios del Concejo de Bogotá

Teniendo en cuenta lo anterior y en entrevista de auditoria se evidencio que se han solicitado en reiteradas oportunidades la adquisición de herramientas y el sistema de detección de incendios para el Concejo de Bogotá y durante dos vigencias no han quedado apropiados los recursos para la contratación a estas solicitudes.

**Evidenciada en el plan de mejoramiento de la vigencia 2016 y se traslada a la Dirección Financiera:**

**p)** Incumplimiento de la norma NTCGP 1000:2009 4.1 Requisitos Generales, 5. Responsabilidad de la Dirección 5.1 compromiso de la Dirección 4.2 Gestión Documental 4.21 Generalidades c) d) 4.2.3 Control de Documentos 4.2.4 control de Registros, 8.5.2 Acciones Correctivas 8.5.3 Acciones preventivas MECI 2014 2.3 Componente Planes de Mejoramiento, Incumplimiento al plan de mejoramiento de la vigencia 2016, se evidencio que las siguientes no conformidades no cumplieron con la realización de las acciones preventivas y/o correctivas

*"NCP 11.2 Si bien en la vigencia 2014-2015 se contrató la empresa PASSWORD para que ayudara la implementación de la norma técnica 27001, no se evidencia acciones por parte de la alta dirección en el 2016 que garanticen implementación y sostenibilidad del subsistema, como es el caso de no tener un oficial de seguridad permanente, no tener establecidas las funciones para el oficial de seguridad, el acuerdo de confidencialidad no ha sido firmado por la gran mayoría de funcionarios (carrera administrativa y provisionalidad y pasantes, entre otros), aun sabiendo que la implementación de este subsistema fue una actividad que quedo sin cumplirse del anterior plan cuatrienal, lo que podría ocasionar un detrimento patrimonial para la Corporación debido a los recursos invertidos. Lo anterior podría generar un posible incumplimiento a las normas ISO 9001: 2008 5.1 Compromiso de la dirección literales d y e, 5.4 Planificación, 5.5.1 responsabilidad y autoridad; NTCGP 1000:2009 5.1 Compromiso de la dirección literales d y e, 5.4 Planificación, 5.5.1 responsabilidad y autoridad; MECI 2014 1.2 Componente Direccionamiento Estratégico la acción propuesta 1: implementar la norma técnica 27001 y garantizar su sostenibilidad.*

Seguimiento: *si bien se presentó la ficha técnica para contratar la implementación de la norma ISO 27001 en febrero de 2016 al director administrativo, así como que el director financiero a través de memorando IE9092 informa que para la vigencia 2016 no quedaron apropiados los recursos para el mantenimiento, mejora y certificación del Sistema de gestión de seguridad de la información, y a la fecha de la auditoría practicada en la vigencia 2017,se observa que aún no se ha contratado a nadie que apoye dicha implementación y practique la auditoria para certificación.* ***CONTINÚA ABIERTA.***

*NOTA: Esta No Conformidad Potencial se le da traslado a la Dirección Financiera para que garantice la contratación en la presente vigencia en cuanto a la certificación e implementación de la norma ISO 27001,*

**<u>Evidenciada en sistemas y seguridad de información y es trasladada compartida con la oficina asesora de planeación</u>:**

**q)** De acuerdo al plan de acción aprobado mediante resolución 333 del 16 de Mayo de 2017, se realizó una revisión de las actividades que están bajo responsabilidad del proceso de sistemas y seguridad de la información que se encuentra publicado en la red interna de la Entidad, a través del link de Planeación y se identificaron los siguientes aspectos que podrían llegar a presentar incumplimiento de la realización de las actividades allí descritas tales como:

| | | | |
|---|---|---|---|
| **12- Sistemas y Seguridad de la** | 26 | Proveer un servidor | Plataforma Tecnológica Actualizada Adquisición de Hardware |

**Información**

| | | |
|---|---|---|
| 27 | Proveer o actualizar licencias para el Servidor | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| 28 | Proveer licenciamiento de Correo Electrónico | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| 29 | Proveer un sistema de seguridad y protección de Amenazas de Red | Plataforma Tecnológica Actualizada Adquisición de Software |
| 30 | Proveer 45 portátiles para el Concejo | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| 31 | Proveer un software para monitoreo de Red y Servidores | Plataforma Tecnológica Actualizada Adquisición de Software |
| 32 | Proveer el sistema de streaming de Audio y Video | Plataforma Tecnológica Actualizada Adquisición de Software |
| 33 | Proveer un software para Diseño Grafico | Plataforma Tecnológica Actualizada Adquisición de Software |
| 34 | Adición y prorroga al contrato 160304 de 2016, servicios técnicos que garanticen el correcto funcionamiento de la Librería de Backups LTO 7 | Plataforma Tecnológica Actualizada Adquisición de Software |
| 35 | Proveer un sistema de Red Inalámbrica. | Plataforma Tecnológica Actualizada Adquisición de Hardware |
| 36 | Adquirir soluciones tecnológicas Integrales para el Concejo de Bogotá. Realizar trámites para la adquisición del sistema de Voto Electrónico del Recinto de los Comuneros en materia de Sonido, y demás Tecnologías para la realización de las sesiones de los Honorables Concejales. | Recinto los Comuneros adecuado en materia de sonido y voto electrónico. Renovación del sistema de voto electrónico por obsolescencia tecnológica , el actual sistema cumplió su vida útil |

De acuerdo a las actividades anteriormente registradas en el cuadro, se encontraron las siguientes observaciones a tener en cuenta:

Actividades 26, 27, 28, 29, 30, 31, 32, 33, 34, 35 y 36. Proveer un servidor, Proveer o actualizar licencias para el Servidor, Proveer licenciamiento de Correo Electrónico, Proveer un sistema de seguridad y protección de Amenazas de Red, Proveer 45 portátiles para el Concejo, Proveer un software para monitoreo de Red y Servidores, Proveer el sistema de streaming de Audio y Video, Proveer un software para Diseño Gráfico, Adición y prorroga al contrato 160304 de 2016, servicios técnicos que garanticen el correcto funcionamiento de la Librería de Backups LTO 7, Proveer un sistema de Red Inalámbrica. Adquirir soluciones tecnológicas Integrales para el Concejo de Bogotá. Realizar trámites para la adquisición del sistema de Voto Electrónico del Recinto de los Comuneros en materia de Sonido, y demás Tecnologías para la realización de las sesiones de los Honorables Concejales.

Se observa que las anteriores actividades de proveer estos recursos no están en cabeza del proceso de sistemas de seguridad de la información, sino son responsabilidad directa

de la Dirección financiera a través de fondo cuenta, por tanto la actividad debería establecerse o describirse como realizar el trámite de la solicitud mediante ficha técnica, según estudios IT del concejo de Bogotá. Lo anterior podría generar un incumplimiento del plan acción 2017, toda vez que como ha sucedido en vigencias anteriores, el proceso de sistemas realiza todos los tramites pero la consecución de los recursos no se realiza a tiempo o simplemente no se realiza la contratación y el cumplimiento de la actividad quedaría en cero 0% de ejecución. Por tanto se observa que la descripción de la actividad no corresponde a la gestión propia del proceso de sistemas y seguridad de la información.

De otra parte, a continuación se muestra el cuadro que corresponde a los indicadores de gestión del proceso de sistema y seguridad de la información que hace parte integral del plan de acción 2017.

| | | | |
|---|---|---|---|
| **12- Seguridad y Sistemas de Información** | 92 | Tramitar todas las solicitudes de contratación referente a la plataforma tecnológica del Concejo de Bogotá D.C. | Plataforma Tecnológica actualizada |
| | 93 | Planificar y Realizar las encuestas de satisfacción de los usuarios con relación al Proceso y Subsistema de Sistemas y Seguridad de la Información | Soporte en la implementación del Subsistema de Gestión y Seguridad de la Información y Calidad de la Sostenibilidad del Procesos |
| | 94 | Dar soporte en software, aplicativos, hardware, a través de la mesa de ayuda del proceso de sistemas y seguridad de la información. | Soporte y Asistencia de Calidad tanto en software como hardware para mejorar la integridad de los servicios tecnológicos. |
| | 95 | Realizar las copias de seguridad de la información del Concejo de Bogotá D.C. | Medir la eficiencia y eficacia en la realización de copias de seguridad y de respaldo de la información, de conformidad con el Subsistema de Gestión y Seguridad de la Información |

Conforme a estas actividades se observa lo siguiente:
Actividad N. 92: Tramitar todas las solicitudes de contratación: esta labor estaría inmersa en la gestión que se adelantaría en el primer cuadro con los trámites para garantizar la compra de los recursos tecnológicos, con respecto a las actividades 93, 94 y 95 no se realizan observaciones al respecto.

Por otra parte, se observó que en el plan de acción de la vigencia 2016, se habían establecido las siguientes 2 actividades que estaban relacionadas con la creación de la Dirección de tecnologías y sistemas de información asi:

| | | | | | |
|---|---|---|---|---|---|
| 18 | Solicitud de concepto de viabilidad técnica y presupuestal para la creación de la Oficina de Relaciones Internacionales y la Oficina de Sistemas y Tecnólogias. | Conceptos emitidos por las entidades competentes | 100,00% | 18 | (Conceptos emitidos / Conceptos solicitados ) *100 |
| 19 | Presentación del Proyecto de Acuerdo para la creación de la Oficina de Relaciones Internacionales, de la Oficina de Sistemas y Tecnologías, y la creación de los cargos de la Oficina de Relaciones Internacionales y de la Dirección de Tecnologías y Sistemas de Información [Dec. 415-2016 DAFP]. | Armonización del trabajo con los lineamientos de Mintrabajo y MinTIC. | 100,00% | 19 | Presentación Proyecto de Acuerdo para aprobación de la Nueva estructura del Concejo de Bogotá D.C. |

De lo anterior se observó que durante toda la vigencia 2016, nunca se dio cumplimiento a la ejecución de estas actividades, ni los conceptos emitidos, ni la presentación del proyecto de acuerdo para la creación de esta y para el plan de acción 2017 no quedo establecido en ninguna actividad la creación de la dirección de tecnologías y sistemas de información, teniendo en cuenta que el Decreto 415 del 7 de marzo de 2016, en sus Artículos 2.2.35.4 Nivel organizacional y 2.2.35.5 Roles, establece que la entidad debe contar en su estructura con una dependencia encargada del accionar estratégico de las tecnologías y sistemas de información y las comunicaciones, el cual hará parte del Comité Directivo y dependerá del nominador o representante legal de la misma. Asi como los roles que el director, jefe de oficina o coordinador debe cumplir.

Las anteriores observaciones se recomienda sean tenidas en cuenta para evitar un posible incumplimiento de la norma NTCGP 1000:2009 4.1 Requisitos Generales, literal c, d, e, f y g 5. Responsabilidad de la Dirección 5.1 compromiso de la Dirección 4.2 Gestión Documental 4.21 Generalidades c) d) 4.2.3 Control de Documentos, literal a y b 4.2.4 control de Registros, Numeral 5.4 Planificación, 5.6 revisión por la dirección. MECI 2014 Modulo de control de Planeación y Gestión, Componente Direccionamiento Estratégico, Elementos: Planes, Programas y proyectos.

## 13. CONCLUSIONES

Realizada la auditoria al proceso de Sistemas y Seguridad de la información, se observó que se realizaron la mayoría de las acciones tanto preventivas como correctivas establecidas en el plan de mejoramiento de la vigencia 2016, así mismo se requiere que las no conformidades pendientes de ejecución se realicen antes de que termine la presente vigencia y no quede nada pendiente para el próximo año y evitar consecuencias disciplinarias por incumplimiento de dos vigencias de las acciones establecidas, con relación a lo observado en la auditoría practicada en la presente vigencia 2017, se observa que el proceso viene cumpliendo con la gestión propia, quedando aspectos

relacionados en el presente informe pendientes por ajustar, actualizar o cambiar.

14. RECOMENDACIONES

**14.1** (11.1). Se recomienda tener en cuenta los aspectos identificados por la oficina de control interno para mejora y actualización del proceso sistemas y seguridad de la información.

**14.2** (11.2). Se sugiere realizar todos los cambios a que haya lugar en los procedimientos adscritos al proceso teniendo en cuenta todas las observaciones dadas en el presente informe definitivo.

**14.3** (11.3). Se hace necesario realizar los ajustes a la políticas de operación, de acuerdo a la gestión desarrollada.

**14.4** (11.4). Si bien es una no conformidad compartida con el proceso de planeación, es necesario que realicen la solicitud de cambios a través de memorando para ser aprobado en Comité del SIG.

**14.5** (11.5). es necesario realizar todas las actividades para darle cumplimiento a todos los requisitos mínimos que exige la norma 27001, y posteriormente lograr tener la certificación.

**14.6** (11.6). Se requiere que el oficial de seguridad de la información cumpla con todas las actividades que se encuentran bajo su responsabilidad.

**14.7** (11.7). Se recomienda darle cumplimiento a la Resolución 305 de 2008 en los artículos mencionados en el presente informe.

**14.8** (12.2),. Se sugiere ajustar la estructura de personal, conforme a lo establecido en el manual de funciones y competencias de la entidad.

**14.9** (12.3) Se recomienda darle cumplimiento a las acciones tanto preventivas como correctivas establecidas en los planes de mejoramiento.

| EQUIPO AUDITOR | |
|---|---|
| Nombre (s): Ingrid Acosta | Firma (s): |

| JEFE OFICINA DE CONTROL INTERNO | |
|---|---|
| Nombre : Edwin Peña | Firma: |

| FECHA DE ENTREGA | 7-07-2017 |
|---|---|