Radicado DADEP No. RAD_S 20191300031053

Bogotá D.C,
130-OCI

MEMORANDO

PARA: **NADIME YAVER LICHT**
Directora

DE: **ROGER ALEXANDER SANABRIA CALDERÓN**
Jefe Oficina de Control Interno

ASUNTO: Auditoría a protocolos y procedimientos de certificación electrónica en los sistemas de información del DADEP y seguridad de la información.

La Oficina de Control Interno en ejercicio de sus funciones y en especial las establecidas en la Ley 87 de 1993, los roles definidos en el Decreto 648 de 2017, el Plan Anual de Auditoría-PAA 2019-V3, las Normas ISO 27000 de 2018 y 27001 de 2013 y el CONPES 3854 de 2016, se permite presentar el informe del asunto, en los siguientes términos:

1. OBJETIVO Y ALCANCE

Efectuar el análisis, seguimiento y verificación al cumplimiento a lo establecido en el Decreto 1078 de 2015, constatando la seguridad y privacidad de la Información en la entidad. El alcance del presente informe tiene como propósito identificar y delimitar las fallas presentadas en los Sistemas de Información de la entidad, establecer la coherencia y pertinencia del plan de contingencia y su cumplimiento, así como efectuar un comparativo general de la aplicación del Modelo de Seguridad y Privacidad de la Información-MSPI versus el del MSPI en la entidad.

2. CRITERIOS DE AUDITORÍA

- Decreto 1008 de 2018, *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*
- Decreto 648 de 2017, *"Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.*
- Decreto 1083 de 2015, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"*
- Decreto 1078 de 2015, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
- CONPES 3920 de 2018 *"Política Nacional de Explotación de Datos" (Big Data).*
- CONPES 3854 de 2017 *"Política Nacional de Seguridad Digital".*
- CONPES 3701 de 2011 *"Lineamientos de política para la Ciberseguridad y Ciberdefensa".*
- CONPES 3650, de 2010 *"Importancia Estratégica de la Estrategia de Gobierno en Línea".*
- Directiva 005 de 2005 de la Alcaldía Mayor de Bogotá *"Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital".*
- Resolución 305 de 2008 con su respectiva actualización Resolución 004 de 2017, *"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".*

Alexandra Hernandez 2019/10/30 14:05pm

Rec. 30-10-2019 2:00 pm

Recibí ACEA 30/10/2019 2:22pm

30 OCT 2019 1:57

- Circular 095 del 2014 de la Secretaria General de la Alcaldía Mayor de Bogotá y Colombia Compra Eficiente, *"Lineamientos generales para la expedición de manuales de contratación"*.
- Manual de Contratación y Manual de supervisión vigentes del DADEP.
- Guía No. 2 del MINTIC del 2016, *"Elaboración de la política general de seguridad y privacidad de la información"*.
- Guía *"Modelo de Seguridad y Privacidad de la Información"* del MINTIC del 2016.
- Documentación SIG de la Defensoría del Espacio Público.
- Normas ISO 27000 de 2018 *"Vocabulario estándar para el SGSI"*, 27003 de 2010 *"Implementación de un SGSI"* y 27001 de 2013 *"Requisitos para la implantación del SGSI"*.

3. METODOLOGÍA DEL ANÁLISIS

La auditoría adelantada se encontraba programada desde el Plan Anual de Auditoría-PAA V1, aprobado por el Comité Directivo del 31 de enero con un alcance más amplio que incluía lo relacionado con los protocolos y procedimientos de certificación electrónica, sin embargo, por solicitud de la Dirección y debido a los incidentes ocurridos en la Oficina de Sistemas, en la versión 3 del PAA, fue adelantada su ejecución y se encaminó principalmente a la seguridad de la información; por lo que el análisis de los temas señalados en un principio quedará para la vigencia 2020.

En el presente seguimiento y verificación, se tomó como origen la información suministrada del Proyecto de Inversión 1122: *"Fortalecimiento de la Plataforma Tecnológica de Información y Comunicación"*, a través de la Oficina de Sistemas-OS, la Subdirección Administrativa, Financiera y de Control Disciplinario-SAF y CD, la Oficina Asesora de Planeación-OAP y la Oficina Asesora Jurídica-OAJ.

En respuesta al memorando con radicado No. 20191300023993 del 2 de septiembre del 2019, en el cual se da apertura a la auditoría, esta oficina procedió a validar la información puesta a disposición por la Oficina de Sistemas-OS, en la carpeta pública y por correo electrónico, cotejando con las respuestas suministradas en reuniones de fechas 16 de septiembre y 3 de octubre de la presente vigencia, con el personal encargado y responsable de la ejecución de las actividades en el área. Posteriormente, se verificó el acta del Comité Directivo *"Reunión extraordinaria equipo directivo - problemas en los aplicativos del DADEP"* del 8 de agosto de 2019, en la cual se estableció la necesidad de crear un plan de choque debido a los daños ocasionados en los discos duros.

Por lo anterior, la Oficina de Control Interno programó y realizó la reunión de fecha 4 de septiembre de 2019, con un invitado del MINTIC, el jefe de la Oficina de Sistemas y el responsable directo del tema, con el propósito de contextualizar la información de las posibles causas de los daños ocurridos en el servidor MD3600F (Raid 5 de 21 teras) de capacidad y el servidor SC4020 (con unidad de virtualización de 6 teras).

Seguido del análisis técnico y confrontación de evidencias, a través de pruebas selectivas y aleatorias con el responsable del proyecto, se procede a revisar los planes anuales de adquisiciones, la contratación del proyecto enfocada principalmente a los elementos que sufrieron daño, los ingresos y salidas de almacén. Adicional a lo anterior, se verificó cada uno de los puntos solicitados en el memorando de apertura de auditoría, relacionados con los sistemas de información y la infraestructura tecnológica.

4. ANALÍSIS, RESULTADOS Y OBSERVACIONES.

Es necesario señalar que el contenido de este informe se socializó a la Oficina de Sistemas los días 22 y 23 de octubre, de manera que las respuestas que fueron soportadas, son tenidas en cuenta y forman

parte integral del presente informe. Adicionalmente, se invitó a la Oficina Asesora Jurídica la cual se excusó, por este motivo se le remitió el informe por correo electrónico del 24 de octubre, para que realizaran sus observaciones, sin embargo, las mismas fueron recibidas fuera de término.

Es de resaltar que en el desarrollo de la auditoría se establecen limitantes para su ejecución como: la entrega parcial e incompleta de la información solicitada, el corto tiempo destinado a la verificación, la dificultad presentada en el momento de aclarar dudas con contratistas adscritos a la OS por su ausencia y la dificultad de encontrar la trazabilidad de las solicitudes de adquisición de los componentes de hardware y software, principalmente para la vigencia 2018.

El día 8 de agosto, en desarrollo de un Comité Directivo, el jefe de la Oficina de Sistemas informa acerca de la posible pérdida de información de la entidad, por lo que con base en el acta de dicho Comité a continuación, se relacionan los incidentes presentados que fundamentan el enfoque de la auditoría:

- Se reportaron fallas en los sistemas de información acaecidas el 26 de julio del 2019.
- Se informaron fallas en los servicios el día 28 de julio de 2019, producidas debido a que se alertó 1 disco del servidor de almacenamiento DELL (Es de anotar que con este disco se completó un total de 4 discos alertados, tal como se ve en el reporte de fallas de los sistemas de información relacionado en el numeral 4.3.1 Fallas del servidor, UPS y suspensiones del servicio de los sistemas de información).
- Debido a que no fue reconocido el almacenamiento por el software administrador de la virtualización, se informó acerca de la realización de una reunión el 29 de julio de 2019 con los ingenieros de la Oficina de Sistemas donde tomaron las siguientes decisiones:

  -Utilizar el servidor ODA adquirido en el 2018 para poner en "funcionamiento las aplicaciones de Sicapital".
  -Utilizar el servidor ODA "para configurar la base de Datos Oracle 12C", y migrar la base de datos "de producción de "Oracle 11g que se encuentra en el servidor DELL".
  -Crear en el servidor Oracle Database Appliance (ODA) "los servidores requeridos para el despliegue de las aplicaciones misionales y administrativas".
  -Los ingenieros "líderes de cada aplicativo instalarán, configurarán, y probarán los aplicativos para el paso a producción" de las aplicaciones en el servidor ODA.

- Informaron además que el 2 de agosto de 2019 en horas de la noche se dañó el 5to. Disco del servidor DELL, dejando fuera de servicio todo el almacenamiento, en el que se encontraba la base de datos de producción y los servicios de la entidad.

Frente a los hechos ocurridos, al realizar la indagación por parte de la OCI, se pudo **observar** que la garantía del servidor MD-3600F que presentó fallo sobre los discos se encontraba vencida desde el 17 de enero del 2018, motivo por el cual, el fabricante dejó de emitir parches de actualización y mantenimiento para el mismo.

Es importante mencionar que la auditoría conoció que ya desde el 3 de agosto del 2018, se había suscrito orden de compra 110-00134-30356-0-2018 para la adquisición de la solución Oracle Database Appliance (ODA), para el fortalecimiento de la infraestructura tecnológica de la Defensoría del Espacio Público (Línea 338), que ingreso a almacén (SAF) y salió a la OS con registro No 8290 del 25 de octubre de 2018.

Durante el análisis de los eventos relacionados anteriormente se **observó** que:

- La OS no contaba con un plan de gestión de cambio para la infraestructura tecnológica, que permitiera llevar a cabo la adquisición del servidor de remplazó que alojaba las aplicaciones y bases de datos. Teniendo en cuenta que el servidor DELL contaba con garantía extendida de vencimiento hasta el 17 de enero del 2018 y que las fechas de finalización del soporte del fabricante son publicadas con anterioridad; el proceso de adquisición, gestión del cambio y plan de migración debió contemplarse mínimo desde la vigencia 2017, evitando la materialización de los riesgos.

- El tiempo para lograr que se registrara la orden de compra en la tienda virtual para la adquisición del servidor ODA fue de 6 meses y 14 días, contando desde el inicio de la fecha de vencimiento de la garantía extendida del servidor DELL (17/01/18).

- Desde el 25 de octubre del 2018, fecha de ingreso y salida del almacén del servidor ODA, hasta el 29 de julio del 2019; de acuerdo con las evidencias suministradas por el área, no se logró establecer la gestión realizada para la instalación, configuración y migración de los aplicativos de la entidad de un servidor a otro. Según manifestó el área auditada no se había realizado dada la necesidad de capacitación por la complejidad del manejo del servidor.

- No fueron contratadas las horas de implementación en la adquisición de la compra del servidor ODA, con el proveedor ORACLE COLOMBIA LIMITADA, por lo que la transferencia de conocimiento se realizó mediante manuales de uso, configuración y soporte virtualizado; siendo necesario para esta Oficina, y de acuerdo a la complejidad del uso y apropiación de estas plataformas, que se tenga en cuenta su inclusión en las próximas adquisiciones. De igual forma, se estableció como potencial riesgo que los contratistas son los que han recibido las instrucciones en el manejo de esta infraestructura tecnológica.

- La Oficina de Sistemas, aunque contaba con una maquina ODA en pruebas como servidor de respaldo no previó a tempo la adquisición de los discos de almacenamiento para el servidor DELL MD3600f, que soportara la operación de la entidad.

4.1. Sistema Integrado de Gestión (SIG) y Mapa de Procesos.

El mapa de procesos de la entidad sitúa el proceso de *"Gestión de la Información y la tecnología"*, como un proceso de soporte, que se halla documentado por medio de 3 procedimientos: Mantenimiento y Soporte de la Infraestructura Tecnológica, Seguridad de la Información y Sistemas de Información, cuyo responsable es la Oficina de Sistemas-OS.

Dadas las fallas que se presentaron en los meses de julio y agosto de 2019, se procede a describir las **observaciones** más relevantes en el cumplimiento de los procedimientos adoptados en el Sistema Integrado de Gestión- SIG:

- **Procedimiento de Mantenimiento y Soporte de la Infraestructura Tecnológica**, vigente desde el 12/10/2018, Código: 127-PRCGI-01, Versión 3, cuyo objetivo es: Garantizar la disponibilidad de la infraestructura tecnológica, y el instructivo de "Mantenimiento y Soporte de la Infraestructura Tecnológica", Vigente desde 09/10/2018, código 127-INSGI-02, Versión 3, cuyo objetivo es: Desarrollar las actividades de soporte y mantenimiento para garantizar el correcto funcionamiento de la plataforma tecnológica de la entidad, los cuales se encuentran debidamente documentados, aprobados y socializados:

1. En la documentación publicada en el SIG, se **observó** que el formato 127-FORGI-10 "Control de Acceso al Centro de Cómputo" tiene adjunto instrucciones erradas, las cuales pertenecen a otro formato.

2. Se evidenció el cumplimiento parcial por parte del proceso, respecto al mantenimiento correctivo asistido a través de la mesa de ayuda y documentado mediante el procedimiento de mantenimiento y soporte de la infraestructura tecnológica; sin embargo, se **observó** el incumplimiento del instructivo en el numeral "5. MANTENIMIENTO LA INFRAESTRUCTURA TECNOLÓGICA" por medio del cual se establecen las actividades del *"plan de mantenimiento preventivo de toda la infraestructura tecnológica, de acuerdo a los lineamientos de servicios tecnológicos..."*, que determina *"la dirección de tecnologías y sistemas de la información o quien haga sus veces debe implementar un plan de mantenimiento preventivo sobre toda la infraestructura y los servicios tecnológicos"*; con sus respectivos cronogramas de planeación y seguimiento al cumplimiento del plan, ya que no cuentan con el mismo aprobado y socializado.

- **Procedimiento Seguridad de la Información**, Vigencia desde el 23/11/2018, Código: 127-PRCGI-02, Versión 4, con el objetivo de Garantizar la confidencialidad, integridad y disponibilidad de la información, haciendo adecuado uso de las políticas de seguridad establecidas; documento que se encuentra publicado, aprobado y socializado.

  De conformidad con los incidentes presentados, se **observó** el incumplimiento del objetivo del procedimiento, al no garantizar la integridad y disponibilidad de la información; debido al desconocimiento de la documentación y directrices del proceso aplicadas a las actividades diarias del mismo y los estándares internacionales; situación que permitió la materialización de riesgos, los cuales serán analizados en el numeral 4.2.2 y 5 del presente informe.

4.2 Modelo de seguridad y privacidad de la información-MSPI

Al constatar las actividades determinadas en el seguimiento al plan de trabajo del Modelo, se estableció que las siguientes actividades no fueron cumplidas de acuerdo a la planeación definida así:

4.2.1 Política y manual de seguridad y privacidad de la información.

De conformidad con la Guía No 2 del MinTIC, cuyo propósito principal es crear medidas y procedimientos, que permitan la implementación del MSPI, con el fin de proteger la confidencialidad de la información y su disponibilidad e integridad, se **observó** que, al interior de la entidad, no han sido adoptados mediante Acto Administrativo los instrumentos de la política y manual, incumpliendo lo reglado en el Decreto 1078 del 2015 Único Reglamentario del sector de las tecnologías y las comunicaciones, el Modelo de seguridad y privacidad de la información versión 3.02 del 29/07/2016 MINTIC, y la Guía No. 2 de la Política General MSPI, sin embargo, se encontraron publicadas en el SIG, una vez adoptada la política se debe cumplir con los siguientes numerales de la Guía 2. "Cumplimiento", 3. "Comunicación", 4. "Monitoreo", y 5. "Mantenimiento", pasos que a la fecha no han sido implementados en la entidad.

Al respeto, se revisó la trazabilidad de las actuaciones de las diferentes áreas de la entidad encontrando demoras y dilación por parte de las involucradas al tardar aproximadamente un año en la implementación de los documentos, por lo cual no fue posible la adopción oportuna:

El 10 de diciembre de 2018, el jefe de Sistemas remitió correo electrónico al jefe de Planeación y Jurídica y la subdirectora de la SAF con la siguiente solicitud *"De acuerdo a nuestro Plan de Trabajo y obligaciones de la Ley de Gobierno Digital, adjunto el borrador de la resolución para la adopción de los documentos de "Política de Seguridad de la Información" y el "Manual de Gestión de Seguridad de la Información" con el fin de darle el trámite oficial respectivo"*. El 20 de diciembre de 2018, nuevamente la OS remitió a funcionarios de la Oficina Jurídica, la siguiente solicitud *"Se envía adjunto resolución y formato de inventario de activos de información en formato Excel acerca de la observación del link de transparencia..."*. El 20 de marzo de 2019, el contratista responsable de los documentos de la OS remitió correo al contratista de la Jurídica y al jefe de Sistemas con la siguiente solicitud *"De manera atenta le envió el borrador de la propuesta de la resolución que se realizó en el mes de diciembre pasado sobre la adopción de las políticas de seguridad de la información para que por favor sea revisada y ajustada de acuerdo a los requerimientos necesarios"*, el 22 de abril de 2019 se reitera la comunicación así: *"Le envió adjunto el proyecto de resolución con las observaciones que están más orientadas a la forma"* y posteriormente el 17 de julio de 2019 *"De acuerdo a conversación, le envió adjunto los comentarios sobre el borrador de acto administrativo y los documentos anexos que se mencionan"*.

4.2.2 Comparativo general de la aplicación del Modelo de seguridad y privacidad de la información-MSPI de acuerdo a la norma vigente VS el presentado por la OS de la entidad.

La Oficina de Control Interno, efectuó revisión a los 14 dominios que forman parte de los componentes del MSPI, en el que se **observó** que no se cuenta con:

DOMINIO	OBSERVACIÓN
Políticas de seguridad de la información	Aspecto desarrollado en el numeral 4.2.1 del presente informe.
Organización de la Seguridad de la Información	* El plan de tratamiento de riesgos, el cual se encuentra en construcción, en el que se debe establecer los controles para mitigar, transferir y aceptar los riesgos residuales, debe contar con la matriz de identificación y valoración de riesgos de seguridad digital que es insumo necesario para el plan. Nota: El plan de tratamiento debe ser aprobado por la Alta Dirección de acuerdo con la Guía No 7 de Gestión de Riesgos del MinTIC, que hace parte del MSPI, articulándolo con lo estipulado en el Modelo Integrado de Planeación y Gestión MIPG y la norma ISO 27003 * La socialización de las políticas y el manual de políticas de seguridad de la información, sin embargo, se han dado tips de seguridad de la información haciendo uso del correo electrónico, carteleras digitales y la intranet. * El procedimiento de reporte de incidentes relacionado con la seguridad de la información, entre otros. * Controles en la política para el uso de dispositivos móviles, tales como celulares.
Seguridad de los Recursos Humanos	* Los soportes que permitan verificar la experticia de los contratistas con un nivel de responsabilidad en la seguridad de la información en las diferentes áreas de la entidad. * Con los acuerdos contractuales que permita comunicar al empleado o contratista las responsabilidades de la seguridad de la información protegiendo los intereses de la entidad como parte del proceso de cambio o terminación de empleo, para lo cual deben participar áreas como SAF, OAJ y los supervisores de contrato. * El procedimiento de proceso disciplinario, cuando exista violación a la seguridad de la información.
Gestión de Activos	* La actualización del inventario de activos de información de la vigencia 2019.
Control de Acceso	* La aprobación del manual de políticas de seguridad y privacidad de la información. * La totalidad de los derechos de acceso al (DATACENTER) numeral 4.4 de este informe.
Criptografía	* Mecanismos para la encriptación de la información misional y administrativa de la entidad. * El cargue del Certificado de Sitio Seguro-SSL para el SIDEP 2.0 y el ORFEO. * La verificación de controles de cifrado en otros activos de información de carácter crítico y susceptible de implementar.

DOMINIO	OBSERVACIÓN
Seguridad Física y del Entorno	* Un sistema adecuado para la detección de intrusos, a través de los recursos de red y cibernéticos. * Un procedimiento que establezca la verificación y monitoreo de manera periódica del no uso e ingreso de: equipos fotográficos, de video, audio u otros equipos de grabación, tales como cámaras en dispositivos móviles; identificando los casos que permiten autorizaciones.
Seguridad de las Operaciones	* Procedimientos que permitan verificar la capacidad de la gestión de la demanda tales como: depuración de información obsoleta, tomas de copias de respaldo, depuración para liberar espacio, entre otros. *Las pruebas de copias de respaldo de la información de archivos digitales que hacen parte de los sistemas de información, las que se deben realizar periódicamente y de acuerdo con la política de backups que se debe adoptar en la entidad. * El Fortalecimiento de las pruebas de integridad de los sistemas operacionales, estrategia de retroceso (rollback) antes de implementar los cambios en los aplicativos de la entidad.
Seguridad de las Comunicaciones	* La revisión periódica de los acuerdos de confidencialidad o de divulgación de la información reservada de la entidad. * Acuerdos de transferencia de información.
Adquisición, desarrollo y mantenimiento de sistemas.	* Con un plan de pruebas a los sistemas de información en donde se contemple aspectos relacionados con la seguridad de acuerdo a lo establecido en el aseguramiento del software. * Lo contemplado en la metodología de seguridad en el desarrollo de software de la entidad.
Relaciones con proveedores	* La definición de los riesgos de seguridad a cargo de los proveedores. Para el caso de los proveedores en la nube se debe contemplar los riesgos asociados dentro de entidad. * Los requisitos de acuerdos de niveles de servicio con los proveedores, en cuanto a la seguridad de la información.
Gestión de incidentes de seguridad de la información	* La guía para la gestión de eventos e incidentes de seguridad de la información.
Aspectos de seguridad de la información de la gestión de la continuidad del negocio.	* La planificación formal de continuidad de negocio y recuperación de desastres. * Un análisis de impacto en la entidad de los aspectos de seguridad de la información, que se deben aplicar en situaciones adversas.
Cumplimiento	* Implementación de la transición del protocolo IPv4-IPv6. * El Plan de mejora continua. * La implementación de un Plan de comunicaciones.

Así mismo, se **observó** la existencia en el SIG del Formato Gestión de Riesgos de Seguridad Digital Código: 127-FORGI-24 Versión: 1 vigencia: 30/05/2019, el cual una vez solicitado se entregó bajo la denominación de Matriz de Riesgos de Seguridad de la información, encontrando una inconsistencia, adicionalmente con base en su contenido se evidenció la materialización de los siguientes riesgos: *"Daños ocasionados sobre los equipos del data center y Afectación en el acceso a servicios y sistemas de información por afectación en el fluido eléctrico"*.

4.2.3 Declaración de Aplicabilidad

Una vez revisado el aspecto de la declaración de aplicabilidad, se **observó** que la entidad no lo ha desarrollado, a pesar de encontrarse programado en el Plan del MSPI para cumplimiento en mes de octubre de 2018; al indagar sobre el incumplimiento, el auditado manifestó por correo electrónico del 2 de octubre de 2019, lo siguiente:

"1. El documento no se ha desarrollado debido a que es necesario primero contar con la metodología de gestión de riesgos a aplicar y está ya se encuentra definida en el plan de gestión de riesgos de seguridad digital publicado en el portal web".
"2. Se debe contar con la identificación, análisis y evaluación de riesgos de seguridad digital, los cuales se encuentran aproximadamente en un 70%".
"3. Se debe contar con un plan de tratamiento de riesgos, el cual debe ser revisado y aprobado por comité directivo para su ejecución ya que deben definir recursos, controles o procedimientos para mitigar el riesgo, así como definir qué hacer con el riesgo residual".
Por las razones anteriormente mencionadas, así como lo que propone el estándar **ISO 27003**, es que no se cuenta hasta el momento con el documento solicitado, además de argumentar que el MSPI se viene desarrollando de manera más precisa desde finales de enero del año 2018".

Es importante contar con el desarrollo del documento de Declaración de Aplicabilidad, que contempla los controles que se encuentran implementados, en operación y los que se hayan retirado, de igual manera, se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y las razones del por qué no son requeridas en la entidad). Así mismo, se debe tener en cuenta una medición de la efectividad en donde incluya un registro de cada control, valorando su alcance.

4.2.4 Plan de Recuperación de Desastres

Se **observó** que se cuenta con el *"Manual de Contingencia de las Tecnologías de la Información"* Código 127-MANGI-03 Versión 2 del 10 de junio del 2019, el cual fue remitido por correo electrónico pero no se encuentra publicado en el SIG, y debe ser actualizado posterior a las incidencias presentadas y actualizaciones que a partir de ello se han implementado, puesto que aquí se describen las actividades en forma preventiva con el objetivo que sirvan como guía de acción antes, durante y después de la afectación de un incidente ocurrido. La entidad no cuenta con un Plan de Recuperación de Desastres DRP, siendo necesario para su elaboración el trabajo mancomunado de toda la entidad, contemplando procedimientos (desarrollo de actividades), operaciones (locaciones), recurso humano y tecnológico, entre otros. Por lo anterior, es necesario tener en cuenta para la construcción del DRP la Guía para la preparación de las TIC para la continuidad del negocio del MinTIC en donde indica que dicho plan es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

4.2.5 Capacitaciones realizadas a los profesionales de la Oficina de Sistemas durante el último año y relacionados con el manejo de las aplicaciones de los sistemas de información.

Analizados los soportes de capacitaciones se evidenciaron actas de capacitación dirigidas a algunos profesionales de la OS en inducción y transferencia de conocimiento, en diferentes aplicativos de la entidad como: Sistema Integrado de Gestión, Aplicación SIDEP 2.0, seguimiento a los nuevos desarrollos del SIDEP 2.0, Orfeo, Sistema VUC, SIDEP y Royal; sin embargo, no se evidenció capacitaciones relacionadas con otros sistemas de información como: SIGDEP, SISCO, entre otros, ni las actas o manuales de las plataformas tecnologías que se tienen para el uso de la infraestructura tecnológica de la entidad.

4.2.6 Plan de Backups

En el Manual de Gestión de Seguridad de la Información Código: 127-MANGI-01 versión 2 vigencia 24-10-2018, numeral 5.1.4 "Políticas de Copias de Seguridad" literal b. "Directrices" se establece que la *"Oficina de Sistemas adelantará las acciones administrativas y técnicas requeridas para implementar un proyecto de Datos en la Nube, que sirva como contingencia para los servicios y la información crítica de la entidad", "Los medios de respaldo que vayan a ser eliminados deben ser destruidos de forma adecuada, verificando que no quede la información disponible", "Se realizarán backups de contingencia que serán*

remitidos al archivo central en periodos mensuales y su registro quedará en el formato Control Entrega backups de Contingencia"; etc., analizada su aplicación en desarrollo de la auditoría se pudo **observar:**

- Incumplimiento relacionado con la custodia externa de cintas, sin cumplir con los estándares mínimos de seguridad y de almacenamiento.
- La no entrega por parte de la OS, del informe del estado de los backups que pudieron haber sufrido perdida de información.
- Que a la fecha de los incidentes la OS, no contaba con el plan de backups, situación que ya había sido observado por esta Oficina en el informe *"Seguimiento a lineamientos para preservar y fortalecer la transparencia y la prevención de la corrupción en las entidades y organismos del Distrito Capital"*, con radicado No. 20191300017993, del 4-07-2019.
- Que con fecha del 10-08-2019, se evidenció un documento del Manual de Gestión de copias de respaldo, sin embargo, no se encuentra aprobado ni adoptado.

4.3 Reportes.

En cuanto a mantenimientos de los sistemas de información en el 2019, se evidenció correos internos enviados informando ventanas de mantenimiento, sin embrago, no se **observó** los mantenimientos de los meses de enero, abril, junio y agosto del presente año; no obstante, se cuenta con un patrón y un perfil que apoya las actividades de Arquitectura de Software para la plataforma de SIDEP 2.0. Por lo que es importante que se tenga en cuenta un patrón de arquitectura para los demás sistemas de información propios de la entidad en donde se desarrollen actividades de buena gestión de TI, diseño de buena estructura de datos, definición del código fuente, entre otros, teniendo en cuenta los posibles riesgos a los que se puede enfrentar el grupo de desarrollo.

Con el propósito de verificar la vulnerabilidad de los sistemas, se estableció el análisis de vulnerabilidades llevado a cabo en marzo de 2019 y socializado al interior de la OS, sin embargo, es necesario que se documenten las actividades de remediación frente a las vulnerabilidades que se identificaron y de esta manera se atienda al lineamiento de los Servicios Tecnológicos LI.ST.14 contenida en el documento Lineamientos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI en su versión 1.1 del 17 de mayo de 2017 del MINTIC que indica: *"La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI"*.

De otra parte, se **observó** en los soportes enviados de mantenimiento a los servidores, impresoras, equipos de cómputo, aire acondicionado, UPS, que forman parte de la infraestructura tecnológica, que los reportes generados por los proveedores no cumplen con calidad de información, que permita identificar los posibles cambios generados por el desgaste o tiempo de operación de los equipos.

Adicionalmente, no se cuenta con un plan de mantenimiento preventivo a los equipos de la infraestructura tecnológica entre los que citamos: datacenter, canaletas, wifi, entre otros; incumpliendo lineamiento de los Servicios Tecnológicos - LI.ST.10 Planes de Mantenimiento en el documento Lineamientos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI en su versión 1.1 del 17 de mayo de 2017 del MINTIC en donde: *"La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar un plan de mantenimiento preventivo sobre toda la infraestructura y los Servicios Tecnológicos"*, creando un procedimiento que abarque aspectos del mantenimiento preventivo (como inspecciones regulares, mantenimiento de equipos o sustitución de partes), añadiendo pruebas, análisis y/o monitorización continua, para realizar un diagnóstico, que permita mantener equipos en óptimas condiciones.

4.3.1 Fallas del servidor, UPS y suspensiones del servicio de los sistemas de información:

Fecha	Servicios Afectados	Observaciones
23/01/2019	Se presenta fallo de discos duros en unidad de almacenamiento MD3600f que soporta la operación de las máquinas virtuales de OVM. Previo y paralelo a estos fallos de discos se han venido presentando fallos en el servicio de energía que iniciaron con el daño total de las UPS del DADEP, averiando la UPS dedicada al datacenter y la UPS dedicada a todo el piso de la entidad, es pertinente resaltar que la no protección eléctrica genera e intensifica los errores físicos en los dispositivos electrónicos no ajenos a los que se encuentran alojados en el datacenter como lo son servidores switches PDU librería de cintas almacenamientos, unidades NAS, Firewall y en general todos los dispositivos que se encuentran en el DADEP.	La OCI evidenció en los reportes de fallos que se presentaron los daños de los discos en diferentes fechas en lo corrido del año hasta su falla final, en primer término, en el informe de un fallo presentado por el contratista de infraestructura, en el que se reporta el fallo de 1 disco el día 23 de enero 2019. En Comité Directivo la OS menciona fallos desde el 28 de julio, no obstante, ya había un total de 4 discos alertados. Es de aclarar que no se precisó por parte de la OS, cuando ocurrieron los alertamientos de los primeros discos. La acción correctiva que propone la OS es la adquisición de discos duros, como respaldo de almacenamiento, sin embargo, se evidenció cotización de la empresa CTS Compañía integradora de tecnología y servicios S.A.S, el 1 de febrero del 2019, sin tener en cuenta el vencimiento de la garantía del servidor DELL, desde el 17 enero del 2018. Por lo que no se tuvo previsto discos de respaldo que cubriera la necesidad de manera temporal, mucho antes del vencimiento de la garantía.
09/02/2019	La empresa CTS S.A.S realizo una vista técnica para realizar mantenimiento de la UPS LIEBERT DE 40 KVA modelo AP346, Serial c240524, y banco de baterías de 60 unidades en donde se realizaron las siguientes tareas: se realiza procedimiento de apagado de la ups dejando carga en modo BYPASS, procedemos con el mantenimiento, encontrando que por fallas en el fluido eléctrico constantes en la zona, las baterías y el equipo en general, han sufrido degradaciones graves en sus partes de protección eléctrica, haciendo que su periodo de vida útil se disminuya, se energiza la ups, se da comando de encendido pero la ups presenta falla y no se normaliza el servicio, se deja en modo BYPASS y se pide una ventana de apagado general de la carga. El jueves 14 de febrero, se realiza el apagado total, realizando pruebas en voltajes, conexiones y ajustes de la misma, se resetean alarmas se energiza y queda funcionando correctamente. El 18 de febrero reportan que los ups se pasan de modo on-line a modo bypass, se revisa ups encontrando daño en una bobina del filtro de entrada, cables recalentados por fluctuaciones graves del suministro externo de energía, generando temperaturas excesivas y degradación de algunas de sus partes de protección, se suministra bobina y ventilador para su funcionamiento.	Con relación a la UPS LIEBERT DE 40 KVA: En el reporte realizado por el proveedor de fecha 4 de febrero de 2019, se evidenció que la UPS superó su vida útil de 10 años, y recomienda dar de baja el equipo por obsolescencia tecnológica. También, informó que debido a las fallas eléctricas que se presentan en la entidad se afectó considerablemente su funcionamiento, por lo que se considera urgente la adquisición de la UPS, toda vez que esta se encuentra como regulador de los equipos externos al DATACENTER, con la consecuencia de solo mantener la energía eléctrica por tiempo limitado. Frente a la UPS, marca KEHUA TECH, modelo EA 9915 de 15 KV: En el DATACENTER, se encuentra esta UPS, con fecha de fabricación del 2013, sin respaldo del proveedor por vida útil, con mantenimientos de CTS SAS; UPS que respalda los equipos del DATACENTER por 5 minutos aproximadamente. Por lo anterior, se debe contemplar anticipadamente la modernización de esta UPS.

Fecha	Servicios Afectados	Acciones Correctivas OS	Observaciones OCI
30/06/2019	Todos los sistemas de información y servicios tecnológicos. Se presentó corte del fluido eléctrico en el Edificio por parte del proveedor, ocasionando la no disponibilidad en la totalidad de las redes de comunicación y la infraestructura tecnológica	Luego de identificar el origen del incidente, se iniciaron actividades de recuperación que consistía en encender los servidores físicos y virtuales de aplicaciones y bases de datos.	*Adquirir una UPS con capacidad para mantener el funcionamiento de la infraestructura tecnológica durante un margen de tiempo prudente que genere menores daños sobre los equipos frente a interrupciones no controladas del fluido eléctrico. * Respecto de la línea 367 del PAA versión 8 del 1/03/2019, la OS tenía programado la adquisición de la UPS, sin embrago, hasta el 16/08/2019, se efectúa la solicitud de contratación, transcurriendo 5 meses y 15 días de retraso; a la fecha de cierre de esta auditoría no se encuentra adjudicada la adquisición; evidenciando que se encuentra en la OAJ, con fecha de publicación proyecto de pliego en SECOP II el 10/10/2019.
27/08/2019	ORFEO, página web, intranet y DNS externo. El día 27 se estaba realizando un proceso de copiado de información a un disco con capacidad de 3TB dispuesto para tal fin. Al siguiente día, se evidenció que no se logró terminar el procedimiento y se alertó que el disco estaba lleno, repercutiendo de esta forma en el fallo de encendido del administrador de virtualización de los servicios allí alojados y dejando afectados los servicios antes mencionados. Dell SC4020	Se crearon máquinas virtuales sobre el servidor ODA para empezar a restaurar los servicios afectados, labor que permitió que para el día 29 de agosto en las horas de la noche se restableciera el servicio DNS y página web. EL servicio de Orfeo se logró restablecer para el día 2 de septiembre luego de realizada la respectiva configuración en el servidor virtual dispuesto en el ODA.	* Que de acuerdo con lo manifestado el 20 de Septiembre, por la OS y relacionado con la imposibilidad de evidenciar el porcentaje de almacenamiento, esta oficina considera, que existen varios mecanismos para prevenir la situación presentada como crear snapshots o puntos de restauración en el tiempo, siendo utilizados como un método alternativo, lo cual no requeriría llevar a cabo una reinstalación o configuración de las maquinas o servidores virtuales de algunos sistemas de información que estén contemplados, evitando un reproceso.

De acuerdo a las evidencias encontradas en el reporte de los expertos que acompañaron las incidencias presentadas el 31 de julio, 1 y 2 de agosto y 6 de septiembre, en el servidor DELL de almacenamiento, se **observó** que el experto de la firma SERVETECH, realizó un procedimiento para el restablecimiento de la infraestructura y servicios (reseteo de la máquina), en la que efectuó una serie de procedimientos y configuraciones, sin embargo, no se evidenció medidas de preservación y salvaguarda de la información que se encontraba almacenada en los discos intervenidos, esta situación pudo sobrescribir la información existente, es de anotar que el proceso fue llevado a cabo con autorización del Jefe de la Oficina de Sistemas.

4.4. Datacenter

En relación con el manejo del centro de cómputo se **observó** que:

- Dentro de la documentación del proceso no se encuentra publicado el protocolo referente al ingreso y acceso al centro de cómputo (externos, funcionarios y/o contratistas).

- Si bien se cuenta con un formato de control de visitantes externos al Datacenter, esta Oficina efectuó revisión a la carpeta de registros, observando que no fueron registrados los consultores externos que ingresaron el 8 y 9 de agosto de las empresas RED COMPUTO y CEBP, respectivamente.
- La Oficina de Sistemas no tiene designado un administrador para el software de registro biométrico para el acceso al centro de cómputo, lo que no permite realizar seguimiento a la identificación de los usuarios registrados; horarios de ingreso y salida al centro; depuración y actualización de los funcionarios y/o contratistas que han cambiado sus funciones o actividades; y/o personas que no laboran en la entidad. Esta situación disminuye la postura de seguridad en el acceso a las instalaciones de acuerdo al estándar contemplado en la ISO 27001 en los numerales 11.1.1 Perímetro de seguridad física, 11.1.2 Controles de acceso físico y 11.1.5 Trabajo en áreas seguras.

- Existen deficiencias en el cableado estructurado en el Datacenter, que consisten principalmente en cables sueltos y en estado de deterioro, puertas de los RACKS sin seguridad y abiertas y falta de control en el ambiente y la temperatura del sitio, incumpliendo la "Sección 5.1.9 Política de seguridad física y del entorno del centro de datos" literal "b. Directrices" del Manual de Gestión de Seguridad de la Información, 127-MANGI-01, Versión 2 Vigente desde: 24/10/2018.

4.5. Plan de contingencia.

La Directora de la entidad en Comité Directivo del 8 de agosto de 2019, solicitó con urgencia un Plan de Contingencia, ante el incidente presentado para el arreglo de discos SAN, el cual fue remitido por la OS a través de diferentes correos electrónicos (del 30 de agosto, 5, 13 y 23 de septiembre, entre otros), no obstante, hasta el 23 de septiembre remitieron el Plan de Reacción Contingencia Infraestructura TI DADEP en 14 folios, que contiene 15 puntos relacionados con los incidentes. Esta Oficina de Control **observó:**

- Demora en la entrega del documento consolidado solicitado por la Dirección el 8 de agosto, sin embargo, este se venía presentado fraccionadamente por correo y menciona todas las tareas que se realizaron a la fecha con los diferentes aplicativos y sistemas de información de la infraestructura de la entidad; el plan no ha finalizado y no ha sido completamente efectivo por cuanto a la fecha no se ha podido restablecer el total de los sistemas de información y recuperar a cabalidad la información.

- Concerniente al contenido del documento se encontró improvisación en las actuaciones llevadas a cabo respecto a la configuración de los servidores virtuales sobre el ODA y el DELL, Storage SC4020, al realizarse las configuraciones con limitantes en los recursos de la infraestructura, ocasionando que no trabajen en su capacidad óptima.

- En relación con la información de la base de datos donde se comenta que la perdida de información fue baja y de bajo impacto, se debe entender que fue materializado el riesgo de pérdida de información, ejemplo de ello es la información extraviada del aplicativo CPM relacionada con el Plan de Mejoramiento Institucional que no pudo ser recuperada, generando reproceso al instar a las áreas a recuperar y cargar la información; información contenida en la carpetas públicas de Gestión Documental-GD (faltante de mayo a julio), se realizó la búsqueda en las cintas de back-up pero no se encontró dicha información. La OCI encuentra que no se especifican las actividades ni el tiempo requerido para recuperar dicha información.

- En relación con la información cartográfica del aplicativo SIGDEP, mencionan que continuaran con la restauración, sin embargo, no se evidencian las actividades a llevar a cabo ni el tiempo de duración, entre otros.

- El cronograma enviado por la OS, es orientado al Plan de Migración a la nube, que contempla una serie de actividades orientadas a migrar toda la infraestructura tecnológica de la entidad a la nube que se contratará, estrategia que fue considerada una vez ocurrido los incidentes. Es importante tener en cuenta que la migración en la nube se puede ver afectada por la confiabilidad de su conexión a Internet, si el servicio de Internet sufre interrupciones frecuentes o velocidades bajas, la computación en nube puede no ser adecuada; basarse totalmente en Internet puede ocasionar vulnerabilidad de ataques de hackers, por lo que se debe considerar la identificación basado en el análisis de riesgos de la migración de la información a la nube teniendo en cuenta la estrategia para apoyar todas las actividades que deben ser insumo para la toma de decisiones apropiadas.

Por lo anterior, es pertinente que la OS efectúe un levantamiento de información con todas las demás dependencias, con el fin de establecer a cabalidad que información de los aplicativos, carpetas compartidas, entre otros, no se ha restablecido a la fecha, y de igual forma defina la información que no se recuperará, estableciendo los planes de acción y remediación.

4.6. Plan Anual de adquisiciones-PAA

La entidad en la vigencia 2018 aprobó 50 versiones del PAA con 20 líneas de contratación y en la vigencia 2019 con corte al 25 de septiembre del 2019 ya se contaba con 32 versiones del Plan compuesto por 24 líneas de contratación, para los componentes de software y hardware. En el análisis de la vigencia 2018, se **observó** la eliminación de 3 líneas de contratación, correspondiente a adquisición de dos Switches de red y Patch Panel, que cumplan con las especificaciones definidas en la ficha técnica (línea 339), adición y prórroga a la orden de compra 110-00134-17115-0-2017 (línea 317); y adquirir unidad para tele conferencias que permita la transmisión de audio y vídeo en la sala de reuniones del DADEP (línea 759); y en las otras 17 líneas restantes se **observaron** cambios constantes en la fecha de inicio de las solicitudes de contratación, los objetos y la cuantía.

Para el análisis en la vigencia 2019, se tomó el 100% de las líneas programadas y creadas por la OS en las 32 versiones del PAA, constatando: fecha de programación en el PAA, fecha de inicio de la solicitud, fecha de aprobación de la OAJ y/o SAF, fecha de suscripción de contratos, objetos y cuantía, en las que se identificó:

- Incumplimiento de la programación en el PAA respecto del inicio de la solicitud de contratación, con retrasos entre 2 a 7 meses, de algunos objetos contractuales como: adquisición de disco de almacenamiento para reserva ambiente de prueba, actualización, mantenimiento y soporte de Oracle Database Appliance (ODA), adquisición, actualización y soporte de licencias ArcGis, actualización y soporte del sistema operativo Oracle Linux, Software de virtualización Oracle VM y suscripción Adobe Creative Cloud.

- Demoras en relación con el proceso de adquisición de los discos de más de 2 meses desde la solicitud de elaboración del contrato hasta la fecha de inicio así: solicitud a SAF de no existencia (almacén) del 24/04/2019, CDP #441 expedido el 9/05/2019; posteriormente la OS solicita la elaboración del contrato el 23/05/2019, publicado en SECOP II por la SAF el 12/07/2019, OS solicita el RP el 29/07/2019 y el CRP #613 se emite el 12/08/2019, finalmente se contrata el 1/08/2019 con el contrato 400-00134-448-0-2019, con el proveedor SINGETEL SA de fecha de inicio el 2/08/2019.

- A la fecha de corte de la auditoría el valor de contratación entre software y hardware asciende a $150.123.939 pesos, cifra poco representativa en relación con los recursos asignados para estos componentes.

- No se han comprometido $912.731.061 pesos, a pesar de encontrarse programado y formalizado en las versiones del PAA entre los que se citan: adquisición de impresoras de acuerdo con las características técnicas definidas en la ficha técnica (línea 308); el soporte, actualización y mantenimiento del software de gestión documental Royal/ERDMS; adquisición, soporte y actualización del software de back-up NETVAULT BACK_UP; renovación y soporte de la licencia del software de filtrado para el Firewall FORTINET 500E; actualización del soporte y mantenimiento de las base de datos, DEVELOPER SUITE Y WEBLOGIC ORACLE; y adquisición equipo UPS (Uninterruptible Power Supply) para Datacenter.

  Respecto de la contratación de la UPS, a pesar de encontrarse la recomendación de la Dirección en el Comité Directivo del 8 de agosto, en el que se solicitó: "Celeridad en el proceso de adquisición de la UPS, se evidenció en la trazabilidad solicitada, que la OS el 10/08/2019 llevó a cabo la solicitud de compra ante la OAJ, se realizan varias revisiones y hasta el 10 de octubre de 2019, se publicó el proceso en SECOP II, transcurriendo 38 días hábiles.

- De las 24 líneas de contratación, se eliminaron 11 hasta la fecha de corte de la versión 32 del PAA (25/09/2019) por valor de $265.000.000 pesos; las líneas eliminadas equivalen al 45.8% del total de las líneas planeadas y programadas, entre las que se encuentra la adquisición de actualización de versión de la librería de cintas para copias de respaldo. Adicionalmente una de las eliminadas en la versión 10 del 22-03-2019, se volvió a crear posteriormente con el mismo objeto (Contratar el soporte, actualización y mantenimiento del software de gestión documental Royal/ERDMS). También se aprecian cambios en la cuantía y/o el objeto a contratar en las líneas 307, 308, 313, 321, 322, 367 y 486.

Lo anterior muestra falta de un diagnostico real de necesidades y debilidad en la planeación proveniente de los fallas en los estudios previos (análisis sobre la conveniencia de la contratación y valor estimado) y de mercado; desaprovechando los recursos aprobados y afectando la oportunidad de la contratación, aumentando la probabilidad de materialización de riesgos como los relacionados con vencimientos de licencias y daños o reposición de equipos, como es el caso de los discos de almacenamiento y la adquisición de la UPS.

4.7. Contratación

Mediante correo electrónico del 10 de septiembre de 2019, se solicitó a la OAJ la información relacionada con procesos de contratación llevados a cabo por la Oficina de Sistemas y/o que tuvieran componentes de TIC de la entidad, a lo cual respondieron por medio de correo electrónico del 13 de septiembre, no obstante, se encontraron falencias en la información al no ser registrados todos los datos solicitados de los contratos, como número del contrato, fecha de inicio y terminación, etc.

De la información allegada se pudo establecer que en la vigencia 2018, se evidenciaron 62 procesos de contratación, de los cuales 30 corresponden a contratos con personas naturales tanto de prestación de servicios de apoyo a la gestión (3 con 2 adiciones), como de prestación de servicios profesionales (27 con 14 adiciones); 5 contratos de prestación de servicios con personas jurídicas, uno de ellos adicionado y 10 contratos de compraventa para el componente de software y hardware. Para la vigencia 2019, con corte a 31 de agosto, se habían suscrito 32 contratos, 25 de prestación de servicios profesionales y 1 de prestación de servicios de apoyo a la gestión y 6 a los componentes de la infraestructura (3 de compraventa, 2 órdenes de compra y 1 de prestación de servicios con persona jurídica).

Frente a la revisión llevada a cabo en SECOP II y los expedientes físicos de algunos contratos, se evidenció casos en los cuales se presenta incumplimiento a cargo de la supervisión de los contratos, según lo consignado en el "Manual de Supervisión e Interventoría Código: 127-MANGR-02 Versión: 4, Vigencia desde 30/08/2018, numerales 3.5. Responsabilidades del Supervisor y 4. CAPÍTULO III -

Elementos del Seguimiento y Vigilancia Contractual"; así como, el incumplimiento a la legalidad de las actuaciones contractuales, de conformidad con lo establecido en el Decreto 1082 de 2015, que establece la obligación de la publicación de todos los documentos contractuales, atendiendo el principio de publicidad que rige la contratación en Colombia, entre los que se encuentran:

- Contrato de Compra 400-00131-407-0-2018 Nephix Soluciones Integrales SAS, en SECOP II se encontró que la aceptación de la oferta publicada no se encuentra firmada ni fechada y tampoco se encuentra en el expediente físico.
- Contrato de prestación de servicio 400-00131-408-0-2018 Cluster de Servicios SAS, no se evidencia documentos en el contrato de la etapa precontractual, ni de ejecución en el SECOP II, y en el expediente físico no se encuentra el contrato que ya se encuentra finalizado.
- Contrato de Compraventa 400-00134-285-0-2018 XSYSTEM LTDA, en SECOP II no se evidenció documentos del contrato, ni de la ejecución.
- Contrato de Compraventa 110-00134-302-0-2018 ROYAL TECHNOLOGIES SAS, no aparece en SECOP II.
- Contrato de compraventa 400-00134-448-0-2019 SINGETEL SA, no aparece nada cargado con relación al contrato.

Adicionalmente, en la revisión efectuada a la contratación, se observó que el cuadro evaluativo utilizado por la entidad se encuentra desactualizado por cuanto contempla "Experiencia Específica", que no debe ser considerada en ningún contrato de conformidad con el Decreto 815 de 2018.

De otra parte, pese a que en la mayoría de los contratos de la OS se establece las siguientes obligaciones *"Adelantar las acciones necesarias que garanticen la salvaguarda de la información que se gestione durante la ejecución del presente contrato, informando cualquier situación que generé alteración de la cadena de custodia de la información; Realizar el monitoreo de la infraestructura informática y actuar de manera preventiva para corregir posibles fallos de operación; Realizar un proceso de optimización de los recursos de infraestructura informática existentes, que garanticen la estabilidad de la operación, haciendo más eficiente el uso de los recursos y la distribución del almacenamiento; y Hacer la configuración y migración de servidores cuando se requiera"*, no se **observó** efectividad en el cumplimiento de las mismas, debido a que no hay respaldos constantes, lo que permite inferir que la labor de supervisión no se ha venido realizando adecuadamente, situaciones que derivaron en la materialización de riesgos por los incidentes ocurridos de pérdida de información.

4.8. Información Presupuestal.

De acuerdo con el reporte del PREDIS "información presupuestal para un rubro por fuente de financiación y concepto de gasto-PREDIS" con corte a 31 de diciembre de 2018 del proyecto 1122, se establece que el total de recursos asignados para inversión fue de $2.345 millones de pesos, de los cuales el porcentaje de participación para el componente de adquisición de hardware y/o software (Equipos y licencias) fue del 35.5%, mientas que el componente de gasto de personal contratado para apoyar actividades de fortalecimiento de la gestión institución fue de 64.5%.

CONCEPTO DE GASTO	2018				
	Valor Asignado	% participación	Valor Comprometido	%.Comprometido	% Participación
0112-Adquisición de hardware y/o software	832.117.763	35,48%	822.661.377	98,86%	35,48%
0261-Personal contratado para apoyar actividades de fortalecimiento de la gestión institucional	1.512.882.237	64,52%	1.460.650.254	96,55%	63,52%
TOTAL	**2.345:000.000**	**100,00%**	**2.283.311.631**	**97,37%**	**100,00%**

En la vigencia 2019, con corte a 30 de septiembre de 2019, se establece que el total de recursos asignados para inversión fue de $2.485 millones de pesos, de los cuales el 46.8%, es para el componente adquisición de hardware y/o software (Equipos y licencias); por su parte el componente de gasto de personal contratado para apoyar actividades de fortalecimiento de la gestión alcanzó una participación del 53.2%, como se ve a continuación:

CONCEPTO DE GASTO	2019				
	Valor asignado	% Participación	Valor Comprometido	% Comprometido	% Participación
0112-Adquisición de hardware y/o software	1.162.855.000	46,80%	150.123.939	12,91%	46.79%
0261-Personal contratado para apoyar actividades de fortalecimiento de la gestión institucional	1.322.145.000	53,20%	1.322.145.000	100,00%	53.21%
TOTAL	**2.485.000.000**	**100,00%**	**1.472.268.939**	**59,25%**	**100,00%**

De lo mencionado anteriormente, se **observa** que la mayor parte de inversión se destina a personal y no a la infraestructura tecnológica. Llama la atención que, con corte a 30 de septiembre de 2019, solo se había comprometido el 12.9% de los recursos asignados, ejecución considerada baja en el componente de adquisición de hardware y/o software para este periodo del año, es decir, al cierre del tercer trimestre.

5. ANÁLISIS DE POTENCIALES RIESGOS

La Oficina de Control Interno encuentra que se materializaron los siguientes riesgos.

- Riesgo de vulnerabilidad de la información almacenada en los servidores de la entidad, causado por deficiencias en la capacidad tecnológica de la entidad para soportar los datos almacenados en sus sistemas, desconocimiento de los lineamientos de seguridad de la información, insuficientes controles en los procesos y procedimientos establecidos y deficiencia en la administración de los controles para el acceso a las zonas de procesamiento de información.
- Riesgo por daño en infraestructura tecnológica, originado por la falta de mantenimiento, desgaste de los componentes de hardware y obsolescencia de Software, personal no capacitado en el soporte y mantenimiento de la infraestructura, y uso inadecuado de los equipos.
- Riesgo en la adquisición de software y hardware por no cumplir con las necesidades mínimas requeridas de la entidad; en este caso, ocasionado por la falta de un diagnostico real de la capacidad tecnológica necesaria a contratar, después de trascurrir 10 años de la primera adquisición (servidor DELL), requerimientos incompletos y falta de planeación en el plan de adquisiciones y la contratación.

6. CONCLUSIONES y RECOMENDACIONES.

Como principal conclusión se determina que durante la vigencia 2019, los sistemas de información de la Defensoría del Espacio Público presentaron fallas constantes y/o reiterativas en la prestación del servicio, lo cual trajo consigo desgaste administrativo y reprocesos, así como la pérdida de información institucional, afectando la memoria histórica de la entidad. Esto debido a la falta de gestión en el mantenimiento de la infraestructura tecnológica y la falta de previsión frente a la materialización de diferentes riesgos que ya se encontraban identificados y que por la inexistencia de controles fueron materializados en los términos expuestos en el presente informe, incumpliendo además lo preceptuado en la documentación del proceso contenida en el Sistema Integrado de Gestión.

La auditoría resalta la importancia de continuar con la adopción de los parámetros y requerimientos establecidos en la normatividad vigente en materia de TICs y poner en uso las herramientas necesarias para lograr una adecuada gestión y continuidad de negocio, como la adopción y fortalecimiento del Modelo de seguridad y privacidad de la información- MSPI, la declaración de aplicabilidad, el Plan de Recuperación de Desastres, Plan de Backups, capacitaciones técnicas con transferencia de conocimiento principalmente en cabeza del personal de planta de la entidad, la generación oportuna y de calidad y la atención adecuada a las alertas y reportes presentados y el resguardo y protección física de la infraestructura.

Las principales debilidades identificadas en la gestión de la Oficina de Sistemas consisten en que no realizó de forma efectiva la identificación del licenciamiento, garantía y soporte de la infraestructura tecnológica de la entidad, deficiencia de la planeación del cambio en la infraestructura tecnológica de la entidad, fallas en la definición de necesidades, capacidad y escalamiento para la plataforma que soporta los procesos, falta de gestión que afecta la oportunidad en los tiempos establecidos para la adquisición e implementación de software y hardware y falencias en la aplicación del plan de contingencias.

También se concluye falta de celeridad en los procesos de contracción desde el radicado de la solicitud hasta la firma del contrato o publicación por parte de las dependencias involucradas en el proceso contractual, como fue el caso de la UPS y los discos de almacenamiento.

Faltando 2 meses para el cierre de la vigencia presupuestal, la Oficina de Control Interno genera una alerta de riesgo de incumplimiento de la ejecución asignada a la Oficina de Sistemas por valor de $1.800 millones de pesos, en los que $1.697 millones de pesos, corresponden al componente de-Adquisición de hardware y/o software; con las consecuencias tanto de orden administrativo de organismos de control, como sanciones presupuestales por parte de la Secretaría Distrital de Hacienda.

Con base en las observaciones desarrolladas en el informe y las conclusiones presentadas, la Oficina de Control Interno **recomienda:**

1. Aplicar la normatividad el MSPI, lineamientos y directrices en materia de la TICs, adoptando las herramientas necesarias tales como la declaración de aplicabilidad, el DRP, el plan de Backups o copias de respaldo teniendo en cuenta que se deben someter a pruebas periódicas.

2. Fortalecer la gestión de los riesgos debido a su materialización, de manera que se requiere volver a evaluar los riesgos propios del proceso y la criticidad asociados en la matriz de riesgos de gestión y de seguridad digital, estableciendo el apetito por el riesgo y definiendo los lineamientos para su monitoreo y seguimiento; actividad que debe ser realizada de forma inmediata.

2. Hacer una verificación técnica previa a las adquisiciones de los sistemas de información respecto de la compatibilidad de hardware y su escalabilidad, garantizando la efectiva cobertura de las necesidades con base en estudios de mercado que redunde en el fortalecimiento de la planeación contractual.

4. Tener en cuenta la situación a la que se ve abocada la entidad en el cambio de administración con el presupuesto requerido para el sostenimiento de la plataforma tecnológica en la nube, que tiene como propósito migrar los sistemas de información y servicios tecnológicos; previendo desde este momento una alternativa que permita en forma oportuna lograr el almacenamiento de la información.

5. En el plan de recuperación de desastres, describir las acciones necesarias a ejecutar para la activación del DRP en el centro de datos del DADEP, con el fin de respaldar las aplicaciones críticas bajo la modalidad que se disponga, asegurando, la continuidad de la operación ante un desastre o contingencia e iniciar con el correcto funcionamiento de los servicios identificados como críticos por la entidad, así como garantizar la seguridad del Datacenter.

6. A las distintas áreas involucradas en el proceso de contratación en sus distintas etapas, propender por la oportunidad, agilidad y diligencia en los trámites necesarios para llevar a buen termino cada uno de los contratos suscritos en la entidad, dando cumplimiento al PAA, evitando así sus modificaciones y la generación de diferentes versiones durante la vigencia, así como la unidad y completitud de los expedientes contractuales y las publicaciones en el SECOP.

7. A la Alta Dirección solicitar el informe de resultados de la aplicación del Plan de contingencia por parte de la Oficina de Sistemas, donde se puntualice el estado actual de la pérdida de información y las posibilidades y tiempos para la recuperación efectiva de la misma, así como para la normalización definitiva de los sistemas de información.

   Tomar las medidas pertinentes para garantizar que las diferentes áreas o dependencias colaboren en la recuperación de la información y determinar la necesidad de pronunciarse ante los administradores del edificio y el prestador del servicio de energía por los constantes cortes que ocasionan daños en los equipos tecnológicos y la no disponibilidad en las redes.

   Analizar la posibilidad de contratar un proceso de auditoría externa, de ser posible con enfoque forense (teniendo presente que esta se pudiera ver afectada en sus resultados debido a la manipulación de los equipos, tal como se evidenció en las actividades consignadas en el informe) que diagnostique y determine el estado actual y de necesidades de la infraestructura tecnológica para el cumplimiento del objeto misional de la entidad y finalmente, determinar la procedencia de iniciar procesos disciplinarios que se desprendan de las actuaciones de funcionarios y/o contratistas.

NOTA: Las observaciones y recomendaciones presentadas por la Oficina de Control Interno en sus informes tienen como fin último generar valor para la Defensoría del Espacio Público, contribuyendo al logro efectivo de los objetivos misionales a través de la mejora continua de los procesos, por esta razón, se espera sean consideradas por los responsables, a quienes se conmina a la realización de los ajustes, correcciones o mejoras a que haya lugar, y a incluirlas en el aplicativo CPM y gestionarlas de manera adecuada, oportuna y preventiva, ante la posible

Adicionalmente, es de gran importancia comprender que dada la magnitud de la información, lo evaluado, observado, recomendado y demás aspectos señalados en los informes por esta Oficina, tienen fundamento en verificaciones y revisiones realizadas sobre muestras seleccionadas con técnicas de auditoría, es decir, no es posible cubrir el cien por ciento del universo, por lo cual los responsables de los procesos y la Alta Dirección deben tener presente el autocontrol y considerar la existencia de riesgos en dentro de la información no seleccionada, para lo cual es factible pensar en extrapolar los posibles efectos, controles y correctivos sugeridos para la muestra sobre el total del universo.

Cordial saludo,

ROGER ALEXANDER SANABRIA CALDERÓN
Jefe Oficina de Control Interno

Proyectó: Fernando A.Salgado T. y Gina E. Gómez R.
Revisó y aprobó: Roger Alexander Sanabria Calderón
Fecha: 28-10-2019
Código: 1308515

Copia: Julio Alexander Hernández, Jefe Oficina de Sistemas
Isaías Sánchez Rivera, Jefe Oficina Asesora de Planeación
Janeth Caicedo Casanova, Jefe Oficina Asesora Jurídica
Marelvi María Montes Arroyo, Subdirectora Administrativa Financiera y Control Disciplinario