Radicado DADEP No. 20181300017003
20181300017003

Bogotá D.C, 22-05-2018

MEMORANDO

PARA: **NADIME AMPARO YAVER LICHT**
Directora

DE: **ROGER ALEXANDER SANBRIA CALDERÓN.**
Jefe Oficina de Control Interno

ASUNTO: Auditoría al Proceso Gestión de la información y la tecnología.

En cumplimiento a las funciones definidas en la Ley 87 de 1993, los roles establecidos en el Decreto 648 de 2017 y al Plan Anual de Auditoria (PAA-2018), la Oficina de Control Interno realizó auditoría al proceso de Gestión de la Información y la Tecnología y específicamente a los tres procedimientos asociados a este, como son:

- Mantenimiento y soporte.
- Seguridad de la información.
- Sistemas de información.

Cabe resaltar que los procedimientos evaluados están directamente relacionados y son operados por la Oficina de Sistemas, en desarrollo del componente tecnológico de la Entidad; a continuación se presentan los resultados obtenidos:

1. OBJETIVO Y ALCANCE

El proceso de auditoria se enmarcó en la revisión del cumplimiento de lo definido en los documentos oficializados y publicados en la plataforma del Sistema Integrado de Gestión-SIG de la Defensoría y su correspondiente aplicación en las actividades estratégicas, misionales y de apoyo.

2. METODOLOGÍA

La revisión inicia con la validación de los documentos cargados y oficializados en el SIG y convalidando a través de reuniones y revisiones con el personal encargado y responsable de la ejecución de las actividades dentro de la Oficina de Sistemas.

Al finalizar el trabajo de campo, se socializó el informe preliminar el día 8 de mayo al Jefe de la Oficina de Sistemas vía correo electrónico, con el fin de recibir comentarios y realizar ajustes al informe final; posteriormente, el día 16 de mayo se recibe retroalimentación a las observaciones por parte del Jefe de la Oficina de Sistemas de igual manera vía correo electrónico las cuales hacen parte integral de este informe y se incluyen en el numeral correspondiente de la observación.

3. ASPECTOS POSITIVOS

A continuación se mencionan temas observados en el trabajo de auditoria, considerados fortalezas, indicando gestión por parte de la Entidad:

- Los documentos sujetos a evaluación se encuentran cargados correctamente sin presentar errores de apertura en la plataforma del SIG. Al respecto, en las ultimas vigencias se han creado nuevos documentos, manuales, políticas e instructivos, permitiendo un adecuado desarrollo, fortalecimiento y cumplimiento del sistema.

- Para el uso de los formatos, se observa una alineación con la política de cero papel, siendo estos almacenados y organizados en las carpetas electrónicas que la Oficina de Sistemas administra.

4. RESULTADOS Y OBSERVACIONES

Se realizó revisión de los procedimientos asociados al proceso de Gestión de la Información y la Tecnología directamente relacionados con la Oficina de Sistemas de la Entidad relacionados a continuación:

Plan PETIC	1
Caracterización de proceso	1
Procedimientos	3
Formatos	8
Instructivos	2
Guías	2
Directriz	1
Política de Seguridad de la Información	1
Manuales	1

A continuación, se presentan las observaciones determinadas en el proceso de evaluación:

4.1 Actualización de documentos publicados en el SIG

En la siguiente tabla presentamos el inventario de documentos asociados al proceso con las fechas de emisión o últimas fechas de modificación, con el fin de conocer el tiempo que llevan publicados sin haber realizado actualizaciones o modificaciones.

DOCUMENTO	FECHA PUBLICACIÓN O ÚLTIMA ACTUALIZACIÓN
Plan Estratégico de las Tecnologías de la Información	14/11/2017
Proceso Gestión de la Información y la Tecnología caracterización	05/10/2015
Formato Control de Acceso al centro de computo	27/06/2016
Formato Único de Sistema	29/12/2016
Instructivo Mantenimiento y Soporte de la Infraestructura Tecnológica	29/12/2016
Procedimiento Mantenimiento y Soporte de la Infraestructura Tecnológica	29/12/2016
Directrices para manejo de las TICs	28/04/2014
Formato Compromiso de buen uso de los sistemas de información del DADEP- Usuarios externos	05/09/2016
Formato Control de Entrega Backups de Contingencia	25/04/2016

DOCUMENTO	FECHA PUBLICACIÓN O ÚLTIMA ACTUALIZACIÓN
Guía Seguridad de la Información	20/10/2015
Manual de Gestión de Seguridad de la información	19/10/2017
Política de Seguridad de la Información	19/10/2017
Procedimiento Seguridad de la Información.	28/04/2014
Formato Creación de Terceros Contratistas o Proveedores	28/04/2014
Formato de control de cambios Tecnológicos	30/08/2017
Formato Solicitud de Información o Modificación a la Base de Datos de los Sistemas de Información	28/04/2014
Guía Sistemas de Información	30/08/2017
Instructivo Administración de la base de datos geográfica, administración, actualización y mantenimiento del mapa digital del DADEP.	28/04/2014
Procedimiento Sistemas de Información	30/08/2017
Requerimientos de Sistemas de Información	20/11/2016

Es preciso armonizar y articular toda la documentación del proceso, teniendo en consideración que por ejemplo, del procedimiento de seguridad de la información en la vigencia 2017 se creó la política y el manual de gestión de seguridad de la información sin haber modificado y/o actualizado el respectivo procedimiento que aparece con fecha de actualización del 28 de abril de 2014, de manera que la información contenida en el procedimiento, no contempla el uso del formato actualizado.

Respecto a este tema la Oficina de Sistemas responde que en lo referente al ítem 4.1 titulado actualización de documentos publicados en el SIG, estos serán actualizados de conformidad con una acción de mejora planteada.

4.2 Incumplimientos de las actividades descritas en los procedimientos dentro del SIG.

Se realiza barrido de los documentos asociados a cada uno de los procedimientos relacionados con el ámbito tecnológico, para los cuales se observan incumplimientos de lo definido. A continuación, se presentan los casos discriminados por procedimiento:

4.2.1 Procedimiento de mantenimiento y soporte

4.2.1.1 Instructivo Mantenimiento y Soporte de la Infraestructura Tecnológica

- Según el numeral 4.4 titulado "Como solicitar asistencia a la MDA", uno de los medios registrados consiste en el reporte de solicitudes vía web por medio de la herramienta de mesa de ayuda http://mesadeayuda.dadep.gov.co. Y sobre la cual se registra de manera automática la solicitud, el cual es revisado por un agente de mesa de ayuda. Como prueba se ingresa al vínculo mostrando conexión a la herramienta GLPI. Al intentar realizar autenticación con el usuario de la red, la aplicación no permite el acceso, de manera que este medio no está operando actualmente; como complemento se consulta a la mesa de ayuda de cuantas solicitudes han ingresado por este canal obteniendo como resultado 0 solicitudes.

- En el numeral 4.7 se describen las instrucciones para la gestión de incidentes y requerimientos radicados en la MDA; la actividad número 4.7.1 menciona en la nota al final de la instrucción la existencia del instructivo con las indicaciones de cómo crear un caso en mesa de ayuda a través de la herramienta de gestión. Al revisar el vínculo en la intranet, y descrito en el instructivo, no se visualiza el documento mencionado.

4.2.2. Procedimiento seguridad de la información

4.2.2.1 Guía de seguridad de la información

- En el numeral 4.1.2. se describe la mitigación a la amenaza de los hackers presentando el diagrama del mapa de red de la Defensoría desactualizado, informando que el documento data de octubre de 2015. Desde la fecha de emisión hasta la presente vigencia, se han presentado actualizaciones en la infraestructura tecnológica tales como la cantidad de VLAN, unificación de impresoras y equipos de cómputo en la misma VLAN y eliminación del componente portal cautivo entre otros.

- También, en el componente de red WIFI se menciona que para la conexión de los usuarios, se cuenta con el portal cautivo, no obstante al validar esta actividad, se menciona que actualmente no está operando dicho portal, ya que las conexiones se realizan entre los dispositivos móviles y los puntos de acceso a la red WIFI controlando la conexión por medio de un password el cual es administrado por la Oficina de Sistemas.

4.2.2.2 Manual De Gestión de Seguridad de la Información:

- Numeral 5.1.1 Política de Correo Corporativo:

  La directriz número 4, relacionada con el correo corporativo define que: "*Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido: El contenido de este mensaje y sus anexos son propiedad del Departamento Administrativo de la Defensoría del Espacio Público, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada. (Privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal.*"

  Al realizar revisión del texto que actualmente se está utilizando en los correos electrónicos de la entidad, se encuentran diferencias en su contenido, a manera de ejemplo se presenta el siguiente:

  "*La información aquí contenida es para uso exclusivo de la persona o entidad de destino. Está estrictamente prohibida su utilización, copia, descarga, distribución, modificación y/o reproducción total o parcial, sin el permiso expreso de la Alcaldía Mayor de Bogotá, pues su contenido puede ser de carácter confidencial y/o contener material privilegiado. Si usted recibió esta información por error, por favor contacte en forma inmediata a quien la envió y borre este material de su computador. La Alcaldía Mayor de Bogotá no es responsable por la información contenida en esta comunicación, el directo responsable es quien la firma o el autor de la misma.*"

- Numeral 5.1.4 Política de Control de Acceso (Usuarios y Contraseñas):

  La directriz numero 8 estipula que "*Las contraseñas deben ser cambiadas cada 30 días y no deben ser escritas en papeles que queden a la vista o en lugares en donde otra persona la pueda encontrar*". Se observa que para el ingreso a la red y para el caso del correo electrónico, la contraseña no está caducando, por tanto, la directriz se está incumpliendo.

- Numeral 5.1.3 Política de Copias de Seguridad:

  La quinta directriz para bases de datos, describe que: "*Para garantizar la continuidad del negocio, en el caso de la base de datos de producción, se requiere hacer una prueba de restauración del backup*

antes de ser enviado a la entidad externa, dejando el registro en el formato Solicitud de Información o Modificación a la Base de Datos de los Sistemas de Información".

Se valida este aspecto con la Oficina de sistemas, quienes informan que los procesos de restauración de un backup se realizan cuando se genera una solicitud por parte de un área o cuando se presentan un inconveniente que reporte el administrador de la base de datos, no obstante, se enfatiza en el incumplimiento de la directriz, dónde se menciona que antes de remitir las copias al ente externo, se requiere realizar una prueba de restauración, actividad que no se está ejecutando actualmente.

De otra parte, en el apartado titulado sistemas de información, la primera directriz define que: "*Se deben generar copias mensuales de las fuentes de los sistemas de información misionales, administrativos y de apoyo a la gestión, una para ser enviada a la entidad externa encargada de custodiar las copias de respaldo y la otra para dejarla en la oficina de sistemas.*". Actualmente, las copias de seguridad remitidas el ente externo (Archivo Distrital) únicamente corresponden a los archivos de bases de datos, sin incluir las fuentes de los sistemas de información.

- Numeral 5.1.9 Política de seguridad física:

En la primera directriz se describe que: "*El ingreso al centro de datos debe ser controlado, para lo cual se debe registrar la planilla Formato Control de Acceso al centro de cómputo, en la que se registra la hora de entrada, hora de salida nombres y motivo de la visita o actividad realizada.*", de acuerdo con lo mencionado, se expresa que la directriz no indica para quienes aplica el diligenciamiento del formato y basado en lo validado con el personal de la Oficina de sistemas, el formato se diligencia únicamente para proveedores o terceros que vienen a realizar labores especificas dentro del centro de datos tales como mantenimientos, inspecciones, instalaciones de nuevos componentes, entre otros; es decir, para ingresos de personal perteneciente a la Defensoría pero no adscritos a la Oficina de sistemas, no se está aplicando la directriz.

Adicionalmente, la quinta directriz menciona que: "*En el centro de datos, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que allí se encuentran.*", no obstante y de acuerdo a inspección física realizada al centro de datos, se observa la existencia de cajas de cartón, equipos y elementos no pertenecientes al espacio, implicando riesgos físicos.

Finalmente, dentro de la sexta directriz, se define que: "*Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control*".

Al validar el tema con la Oficina de sistemas, se informa que para la vigencia 2017 se realizaron 2 procesos de mantenimiento a los detectores de humo y al sistema de extinción, no obstante, desde su instalación en el centro de datos, nunca se han realizado procesos de pruebas, por tanto, no se está observando lo estipulado en la directriz.

- Numeral 5.1.25 Política de gestión de continuidad del negocio:

La directriz número cuatro define que se debe "*Realizar el documento del plan de continuidad del negocio de la entidad.*", al respecto se informa que dicho documento no se ha emitido en la Entidad; asimismo, la directriz número cinco de la policita de gestión de continuidad del negocio describe

sobre las pruebas y simulacros del plan de continuidad del negocio, actividades que no han sido planificadas ni desarrolladas.

Para esta observación la Oficina de Sistemas responde lo siguiente:

1. Referente al ítem 5.1.3: Política de Copias de Seguridad, se realizará la Restauración y Base de Datos como lo recomienda el manual.

2. Referente al ítem 5.1.9: Política de seguridad física, se solicitará a los contratistas del mantenimiento la realización de las pruebas referidas en el la guía y/o se incluirán en el nuevo contrato de mantenimiento. Además, se revisará y se tomarán medidas tendientes a reducir el riesgo, por objetos que no pertenecen al centro de datos.

3. En cuanto al ítem 5.1.25: Política de gestión de continuidad del negocio, la entidad está realizando diversas actividades tendientes a dar cumplimiento a los lineamientos de Gobierno Digital, por lo tanto, la referencia que hace el manual a la Política de gestión de continuidad del negocio, hace parte de los documentos que están pendientes por finalizar, sin embargo; se menciona en el manual porque este debe cumplirse en algún momento, como parte de la implementación de la política de gobierno Digital que la entidad está implementando.

4.3 Observaciones referentes a los formatos catalogados dentro de los procedimientos.

4.3.1 Formato asociado a los procedimientos sin uso.

Dentro del procedimiento seguridad de la información se encuentra definido el formato Compromiso de buen uso de los sistemas de información del DADEP- Usuarios externos, el cual no está siendo utilizado actualmente en la ejecución de las actividades; de igual manera se encontró que este no se menciona en alguno de los documentos asociados al proceso, tales como procedimientos, caracterización, guías, manuales, instructivos y/o políticas.

4.3.2 formatos que no son relacionados en ningún documento (caracterización, procedimiento, instructivo o guía.)

Dentro del SIG, para el procedimiento de seguridad de la información, se tiene catalogado el formato Formato Control de Entrega Backups de Contingencia, el cual esta siendo usado para registrar los envíos mensuales de las copias de seguridad al Archivo Distrital, como una actividad de contingencia, no obstante, no se encuentra registrado en ninguna de las actividades estipuladas en los documentos del procedimiento.

4.3.3 Formato asociado a otro proceso.

El formato Creación de Terceros Contratistas o Proveedores, se encuentra cargado dentro del procedimiento sistemas de información, al validar con la Oficina de Sistemas, fue manifestado que anteriormente, este formato era diligenciado por la Oficina, ya que sobre esta recaía la responsabilidad de la creación de los terceros; de acuerdo con la evolución que los procedimientos han tenido, la tarea de creación de terceros se encuentra a cargo de un profesional de contratación tanto en la Subdirección Administrativa y Financiera-SAF como en la Oficina Asesora Jurídica-OAJ, dependiendo del tipo de contratación.

Respecto a los numerales 4.2 y 4.3, la Oficina de Sistemas responde que se creará una acción de mejora con varias actividades para actualizar los documentos asociados al proceso "Gestión de la Información y la Tecnología" (caracterización, procedimientos, guías, manuales, instructivos y/o políticas) que permitan hacer una sincronización en el llamado a los formatos que se requieran en cada documento, eliminar los que no se estén usando y eliminar actividades que efectivamente no se realicen.

4.4 Desactualización de normograma.

Se realiza revisión del normograma dentro del SIG asociado al Proceso, **observando** desactualización del documento, principalmente de normatividad asociada. A continuación, se relacionan algunas normas o temas que se encuentran regulados y no se han relacionado dentro del normograma:

- 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".
- Directiva 005 de 2005 Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital.
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- Decreto 1078 de 2015 Decreto Único Sectorial del Sector de Tecnologías de la Información y las Comunicaciones.
- Directiva 011 de 2012 de Promoción y uso de software libre en el Distrito Capital.
- Resolución 003 de 2017 "Por la cual se adopta la Guía de sitios Web para las entidades del Distrito Capital y se dictan otras disposiciones".
- Normas asociadas al tema de Derechos de autor como la circula 17 de 2011 y la Directiva Presidencia 02 de 2002.
- Política de seguridad digital.
- Normas asociadas a teletrabajo tal como la 1221 de 2008.
- Documentos CONPES tales como 3920, 3701, 3650, entre otros.

En este aspecto la Oficina de Sistemas informa y aclara que en cuanto al ítem 4.4: Desactualización de normograma, este se envió actualizado a la Oficina de Planeación a comienzos del mes de mayo, no obstante, se revisará para verificar que los documentos mencionados en este ítem estén incluidos.

5. RIESGOS ASOCIADOS.

Con base en los resultados obtenidos en el proceso de auditoría, a continuación, se presentan los siguientes riesgos, que deben ser monitoreados con el fin de evitar su posible materialización:

- Sanciones impartidas por los entes de control debido a los incumplimientos de lo estipulado en el Sistema Integrado de Gestión-SIG de la Defensoría.

- Falta de claridad al momento de la ejecución de las actividades por parte del personal, debido a la desalineación con lo estipulado dentro de los documentos del sistema integrado de gestión SIG.

- Afectaciones en la integridad y confidencialidad de la información principalmente por los incumplimientos de lo establecido frente al tema de backup, así como las debilidades expresadas en el uso y aplicación de las contraseñas.

6. CONCLUSIÓN Y RECOMENDACIONES

Para la vigencia 2017, la Oficina de Sistemas, de acuerdo con el desarrollo de las actividades asociadas, emitió nuevos lineamientos y documentos, complementando y fortaleciendo los procedimientos del proceso de Gestión de la Información y la Tecnología, sin embargo, de manera general se observaron temas tales como desactualización de procedimientos e incumplimientos de actividades registradas permitiendo aumentar la probabilidad de la materialización de los riesgos informados.

Por lo anterior, la Oficina de Control Interno, en pro del mejoramiento continuo del proceso y su impacto en la Defensoría y la Gestión de la Información y la Tecnología, **recomienda** hacer las revisiones, actualizaciones, modificaciones e integraciones necesarias de los procedimientos y su documentación asociada (caracterizaciones, formatos, instructivos, manuales, etc), con el fin de reflejar la realidad del actuar del área en el Sistema Integrado de Gestión.

Es de resaltar el cumplimiento de la política de cero papel, ya que los formatos tienen un flujo electrónico, siendo almacenados y resguardados en los repositorios destinados para tal fin, evitando la impresión física.

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 MAP y gestionarlas de manera adecuada, oportuna y preventiva, ante la posible materialización de riesgos y/o pronunciamientos de los diferentes organismos externos de control.

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 de la Oficina de Control Interno

Copia: **Julio Alexander Hernández Martínez,** Jefe Oficina de Sistemas.

Proyectó: Diego Alexander Urazán Franco
Revisó y aprobó. Roger A. Sanabria Calderón
Fecha. 22-05-2018
Código: 1302201

Mayo 22/18
3.12 p.m.
S.A

22 MAY 2018
3:15 pm