



Bogotá D.C., 01-02-2016

MEMORANDO

PARA: NADIME YAVER LICHT
Directora

DE: WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno

ASUNTO: Informe Preliminar Evaluación de los procedimientos oficializados en el Sistema integrado de Gestión de la Entidad relacionados con tecnologías de la información

La Oficina de Control Interno en cumplimiento de su rol de evaluación y seguimiento y en ejercicio de sus funciones en especial las establecidas en la Ley 87 de 1993 y teniendo en consideración lo dispuesto en los artículos 1°, 2°, 3°, 4° y 12 de la misma norma, realizó una evaluación del cumplimiento y actualización de los procedimientos pertenecientes al proceso de Gestión de la información y la tecnología que estén directamente relacionados con el ámbito tecnológico de la Entidad.

Para tal fin, los siguientes son los procedimientos que fueron revisados dentro del alcance:

- Procedimiento mantenimiento y soporte de la infraestructura tecnológica.
- Procedimiento seguridad de la información.
- Procedimiento sistemas de información.
-

Basado en lo anterior a continuación se presentan las siguientes iteraciones:

I. OBJETIVO Y ALCANCE:

La evaluación tuvo como objetivo principal, la validación de los procedimientos pertenecientes al proceso de Gestión de la información y la tecnología contenidos en el Sistema Integrado de Gestión (SIG)

El trabajo de campo se desarrolló en conjunto con la Oficina de Sistemas.

II. METODOLOGIA

Para el desarrollo de la evaluación, se realizaron reuniones con el personal de la Oficina de Sistemas abordando cada uno de los procedimientos a evaluar.

III. ASPECTOS POSITIVOS Y FORTALEZAS

Ejecutada la labor de auditoría, a continuación se expresan los siguientes aspectos que permiten determinar el grado de gestión que se realiza al tener los procedimientos oficializados en el Sistema Integrado de Gestión de la Entidad, así como también permitieron ser factores críticos de éxito para la evaluación:

- ✚ Las fuentes de información para el proceso de auditoría contenida en la Intranet de la Entidad se encuentra disponible para consulta inmediata.
- ✚ Los formatos Oficiales pertenecientes al proceso de Gestión de la información y la tecnología se están usando actualmente en la ejecución de las actividades desarrolladas por la Oficina de Sistemas.
- ✚ El lenguaje contenido dentro de los procedimientos es entendible evitando el uso de términos y conceptos técnicos que dificulten el entendimiento de los documentos; de igual manera la navegación a través de los documentos es fácil.
- ✚ Las reuniones con la Oficina de Sistemas fueron concertadas con debido tiempo y los cuestionamientos fueron atendidos idóneamente.

IV. OBSERVACIONES Y RECOMENDACIONES

A continuación presentamos las observaciones derivadas del trabajo de auditoría que requieren una intervención por parte de las áreas auditadas por medio de un plan de mejoramiento:

1. Formatos Oficiales del proceso:

Se revisan los formatos oficiales para cada uno de los procedimientos revisados encontrando lo siguiente:

Procedimiento de mantenimiento y soporte de la infraestructura tecnológica:

- ✚ No se tiene asociado ningún formato a este procedimiento dentro del Sistema Integrado de Gestión.
- ✚ Dentro del instructivo mantenimiento y soporte de la infraestructura tecnológica en el numeral 5.1 denominado administración, creación, y eliminación de cuentas de usuarios, en la primera actividad que consiste en el envío de la solicitud por las vías de comunicación establecidas a la mesa de ayuda por parte del Jefe o Subdirector de la Dependencia solicitante, para tal fin se debe diligenciar el **formato solicitud de información o modificación a la base de datos de los sistemas de información**; basado en esto y de acuerdo con la validación realizada, el formato que actualmente se usa para esta actividad es el **Formato Único de Sistemas** el cual también se menciona dentro de la Guía Directrices

para el

manejo de las tics, pero se encuentra catalogado dentro del Procedimiento Sistemas de Información.

Procedimiento Seguridad de la Información:

- ✚ Dentro del procedimiento en el Sistema Integrado de Gestión se tiene incluido el **formato control de entrega de backups de contingencia** pero no se menciona como tal dentro del procedimiento o dentro de la Guía de Seguridad de la Información.
- ✚ En la Guía de Seguridad de la Información, en el numeral 4.1.1 referente al acceso a los servicios tecnológicos, menciona que dentro de los requisitos se debe diligenciar el **formato de solicitud o modificación a la base de datos de los sistemas de información**; cabe resaltar que para los accesos a los aplicativos y a la red de la Entidad se debe diligenciar el **Formato Único de Sistemas**, lo anterior quiere decir que la actividad está llamando equivocadamente el formato que corresponde.

Procedimiento Sistemas de Información:

- ✚ En el Sistema Integrado de Gestión, se tiene catalogado dentro del procedimiento el **formato solicitud de información o modificación a la base de datos de los sistemas de información**, pero este no es mencionado dentro del procedimiento (diagrama de flujo) o de la Guía de Sistemas de Información.
- ✚ Incluido también dentro del procedimiento se tiene catalogado el **formato creación de terceros contratistas o proveedores**; de acuerdo con la validación realizada con la Oficina de Sistemas este formato era usado anteriormente cuando se requería la creación en el sistema de un proveedor o contratista; actualmente esta labor la ejecuta la Oficina Jurídica y debido a eso no es usado dentro del procedimiento de sistemas de información. También se menciona que dicho formato no se encuentra relacionada en la guía de sistemas de información ni en el diagrama de flujo del procedimiento.
- ✚ El procedimiento tiene incluido el **formato único de sistemas** el cual no está contemplado ni en el diagrama de flujo ni en la guía de sistemas de información. Según lo validado, el formato es usado para labores de soporte al momento de crear, eliminar, cambiar y en general administrar las funcionalidades dentro de los sistemas de información de la Entidad.
- ✚ El **formato control de acceso al centro de cómputo** no se menciona en el procedimiento o en la guía y de acuerdo con el personal de la Oficina de sistemas este formato es usado para temas de seguridad.
- ✚ Dentro de la Guía de Sistemas de Información, en el numeral 4.1 se menciona el **formato solicitud de modificación de aplicaciones**, no obstante el mencionado formato no se tienen oficializado dentro del Sistema Integrado de Gestión.

Recomendaciones:

- ✓ Realizar una revisión exhaustiva de los formatos vigentes asociándolos al procedimiento que

corresponda e incluyéndolos dentro de los diagramas de flujo de los procedimientos, para que así exista una referencia y poder hacer trazabilidad y seguimiento a un proceso en general.

- ✓ Para los casos que amerite crear, trasladar, modificar o eliminar los formatos del proceso en el Sistema Integrado de Gestión con la asesoría de la Oficina de Planeación.

2. Actividades o aspectos que difieren respecto a lo registrado en los procedimientos:

Se realiza validación de los procedimientos y a continuación se presentan los siguientes temas que presentan diferencia con relación a lo estipulado en el Sistema Integrado de Gestión:

Procedimiento de Mantenimiento y Soporte de la Infraestructura Tecnológica:

- ✚ Según seguimiento realizado a las actividades descritas dentro del flujograma del procedimiento, únicamente se está tratando el tema de soporte, mas no se cubre el tema de mantenimiento a pesar de que el concepto se usa en un par de actividades.
- ✚ El procedimiento indica en su segunda actividad que se debe registrar el tipo de mantenimiento (preventivo o correctivo) para poder solicitar un servicio. Según lo validado con la Oficina de sistemas, la tipología usada para la creación de tickets en la herramienta GLPI es incidente o solicitud.
- ✚ Dentro del instructivo mantenimiento y soporte de la infraestructura tecnológica, se mencionan los SLA (acuerdos de niveles de servicio) y después de las reuniones sostenidas con la Oficina de Sistemas, respecto al tema fue comentado que estos se encuentran en proceso de estudio y definición.
- ✚ De acuerdo con el diagrama de flujo del procedimiento, en la actividad 5 se menciona que para esta instancia, se da cierre de solicitud en la herramienta de gestión con el consentimiento y evaluación del servicio por parte del funcionario. Esto indica que cada ticket abierto a la mesa de ayuda debe tener una evaluación; al consultar a la Oficina de Sistemas, fue respondido que no se está realizando la evaluación a cada uno de los tickets al momento del cierre sino que se está enviando vía correo electrónico a todo el personal trimestralmente una encuesta de satisfacción, lo anterior presenta diferencia con lo estipulado en el procedimiento.
- ✚ En el numeral 4.4 del instructivo mantenimiento y soporte de la infraestructura tecnológica se mencionan los canales para solicitar asistencia; dentro de los canales mencionados se tiene la web que define el registro de solicitudes por parte del usuario directamente con la herramienta de gestión a través de la URL <http://mesadeayuda.dadep.gov.co/>, no obstante se resalta que los funcionarios y contratistas no cuentan con un id de usuario para hacer solicitudes por este medio; complementariamente se menciona que dentro del instructivo la anterior URL tiene un vínculo al correo mesa de ayuda y no a la página como tal.

Procedimiento Seguridad de la Información:

- ✚ Dentro de la Guía de Seguridad de la Información, se menciona en el numeral 4.1.1

denominado acceso a los servicios tecnológicos la existencia del documento política de seguridad informática del DADEP, no obstante dicho documento no se encuentra oficializado debido a que se encuentra en proceso de construcción.

- ✚ La Oficina de Sistema cuenta con un documento que contiene los lineamientos respecto al centro de cómputo, dicho documento se encuentra sin oficializar y tampoco ha sido incluido dentro del procedimiento o la guía de seguridad.

Procedimiento Sistemas de Información:

- ✚ Dentro del diagrama de flujo del procedimiento, después de la actividad número 3, se genera la pregunta si es un desarrollo propio en la Entidad. Para el caso sí, se ejecuta el requerimiento según lo establecido en la guía y en el caso de no, se documenta y se da a conocer el resultado del requerimiento. Basado en lo anterior no se están contemplando las actividades específicas o la conexión a otros procedimientos para los desarrollos donde sea necesario la contratación de un proveedor, a manera de ejemplo se menciona la Universidad Nacional.
- ✚ Para el desarrollo del SIDEP versión 2.0 se adoptó una metodología de desarrollo de software renovada y para tal fin se va a analizar la posibilidad de incorporarla al Sistema Integrado de Gestión ya que no se tuvo en cuenta el procedimiento existente.

Recomendaciones:

- ✓ Actualizar los procedimientos basándose en el modo de operación actual para que exista concordancia entre las actividades ejecutadas diariamente y lo estipulado en los procedimientos del Sistema Integrado de Gestión, permitiendo una mayor gestión y control del ámbito tecnológico en la Entidad.
- ✓ Específicamente para el procedimiento de mantenimiento y soporte de la infraestructura tecnológica, validar la segmentación de los conceptos de soporte y mantenimiento en 2 flujogramas, ya que cada uno de estos conllevan actividades distintas.
- ✓ Validar que dentro de todos los procedimientos correspondientes a la Oficina de sistemas se contemplen aspectos tales como control de cambios en la plataforma tecnológica, proyectos de TI, sistema eléctrico, telefonía IP, redes inalámbricas, capacitaciones sobre uso de aplicativos, continuidad del servicio y las operaciones entre otros.
- ✓ Para los procedimientos, dentro de los flujogramas en el espacio de formato y registro incluir los nombres de los formatos oficiales con el fin de evidenciar correspondencia entre el procedimiento y los formatos.

V. RIESGOS

Basado en las observaciones en este informe, se presentan los siguientes riesgos:

- No conformidades impuestas por el Ente certificador.
- Incumplimiento de lo estipulado en el Sistema Integrado de Gestión -SIG, de la Entidad.

- Desconocimiento del SIG.
- Falta de claridad en las directrices establecidas.
- Falta de integridad y consistencia en la información del proceso dentro del SIG.

VI. OTRAS OBSERVACIONES

VII.

A continuación se exponen temas, los cuales se consideran de carácter importante que no generan incumplimiento de los procedimientos, mas sin embargo son mencionadas para su conocimiento:

Procedimiento de mantenimiento y soporte de la infraestructura tecnológica:

- ✚ Uno de los canales o medios para solicitar asistencia a la mesa de ayuda es la mensajería instantánea con el icono del sistema spark el cual se usaba anteriormente, por tanto es necesario actualizar el nombre a la herramienta de Gmail.

Procedimiento sistemas de información:

- ✚ En la guía de sistemas de información, se mencionan las diferentes fases de un proceso de desarrollo tales como requerimientos, desarrollo, pruebas y configuración; revisando cada concepto de estos describe con un enfoque teórico la definición y el objetivo cada fase sin embargo no especifica aspectos tales como los entregables de cada una de estas, las actividades propias a desarrollar en cada una de las fases con sus respectivos roles y responsabilidades entre otros.
- ✚ De igual manera en el numeral de actividades a realizar durante el desarrollo de software se menciona que el ingeniero encargado debe definir el modelo lógico de base de datos o modelo relacional del desarrollo junto con el modelo físico de base de datos en donde se describen los campos a crear, junto con el tipo de dato y descripción de cada uno de los campos identificando constrains, llaves primarias y foráneas que puedan existir. De acuerdo con lo anterior, esta es la única actividad definida dentro del procedimiento para desarrollo de software enfocándose principalmente en el tema de base de datos sin describir otras actividades que se realizan durante la fase de desarrollo.
- ✚ Se indaga a la Oficina de Sistemas acerca de la documentación de cada aplicativo basado en el procedimiento de sistemas de información, a lo que se respondió que sería necesario realizar el barrido y la revisión de cada una de las aplicaciones de la Entidad para corroborar cuales soportes documentales existen y cuales serían necesarios construir, para tal fin es recomendable por parte de esta Oficina la validación de la existencia de la documentación exigida para todos las aplicaciones y sistemas de la Defensoría.

VIII. CONCLUSION

Existe un grado de concordancia entre las actividades desarrolladas en el día a día y los lineamientos del Sistema Integrado de Gestión correspondiente al proceso de Gestión de la información y la tecnología, todo esto operado, canalizado y gestionado por parte de la Oficina de Sistemas, mas sin embargo, como aspecto principal y derivado del proceso de auditoría, es importante realizar actualización de procedimientos a nivel general, ya que sobre el ámbito tecnológico en la Defensoría se han presentado cambios significativos en los últimos 2 años, por ende los procedimientos no deben quedar rezagados.

Cordial Saludo,

WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno

Copia: Oficina de Sistemas.
Fecha: Enero 18 de 2016
Proyectó: Diego Urazán Franco
Revisó: William Valderrama Gutiérrez
Aprobó: William Valderrama Gutiérrez