



MEMORANDO

PARA: DANIEL MAURICIO ROZO GARZÓN
Jefe Oficina Tecnología de la Información y el Conocimiento

DE: CAMILO ANDRÉS PULIDO LAVERDE
Asesor de Control Interno

ASUNTO: Informe Final Auditoria Proceso Gestión de Información y Conocimiento

FECHA: Mayo 27 de 2016

Respetuosamente,

Como parte del Rol de Control Interno de "Evaluación y Seguimiento", y en cumplimiento del Programa Anual de Auditoria 2016 Versión 2, atentamente me permito remitir para su conocimiento y fines pertinentes el "*Informe Final de Auditoria realizada al Proceso de Gestión de Información y Conocimiento*"

Agradecemos la atención prestada y esperamos contar con su disposición para adelantar las acciones de mejora a que haya lugar para corregir y prevenir posibles desviaciones y riesgos, el plazo para elaborar y remitir el Plan de Mejoramiento son (10) diez días hábiles contados a partir del recibo de esta comunicación, para la formulación se deberá adelantar lo establecido en el Procedimiento EVG-PD-003 Gestión para la mejora.

La presente auditoria fue desarrollada de acuerdo a las Normas de Auditoria de General Aceptación, sin embargo no constituye una auditoria de Estados Financieros. Cabe resaltar que debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores e irregularidades que no hayan sido detectados bajo la ejecución de nuestros procedimientos de auditoria, previamente planeados. La Unidad, es responsable de establecer y mantener un adecuado sistema de control interno y de prevenir irregularidades.

Agradecemos a cada uno de los funcionarios que hacen parte del proceso por su apoyo en la ejecución de nuestra labor.

Atentamente,



CAMILO ANDRÉS PULIDO LAVERDE
Asesor de Control Interno

c.c. Director General UPRA

Contenido

I. Objetivo

II. Alcance

III. Procedimientos adelantados

IV. Conclusión

V. Riesgos y Controles

VI. Hallazgos y oportunidades de mejora identificadas

VII. Anexos

Firmas de aceptación

I. Objetivo

Evaluar el diseño y la efectividad de los controles existentes en el proceso estratégico – Gestión de Información y Conocimiento, a través de la evaluación de sus riesgos y bajo los parámetros del Modelo Estándar de Control Interno (MECI), para efectos de establecer oportunidades de mejora que procuren el logro de los objetivos del proceso.

II. Alcance

La evaluación se realizó a la gestión adelantada por el proceso entre enero de 2015 y marzo de 2016, contemplando los dominios y/o procesos relevantes de Gobierno y Gestión de las Tecnologías de Información y Comunicaciones y enfocado en los aspectos de ingeniería de software, administración de infraestructura tecnológica, copias de seguridad y soporte y asistencia técnica.

III. Procedimientos Adelantados

La ejecución de la Auditoría estuvo acorde a las etapas y actividades definidas en el memorando específico de planeación del trabajo de Auditoría. Adicional a estas se realizaron las siguientes:

- Entrevista a los funcionarios de la Dirección
- Elaboración y análisis de la Matriz de Riesgos y Controles
- Revisión documental del proceso (Relevamiento del proceso, validación de entregables,)
- Validación de información requerida.

IV. Conclusión

Como resultado de la evaluación realizada al proceso estratégico de Gestión de Información y Conocimiento en lo relacionado a la Gestión de Infraestructura y Gestión de Sistemas de Información y de acuerdo al alcance y objetivos anteriormente mencionados, consideramos que se evidenciaron fortalezas en los siguientes aspectos:

- Elaboración del Plan Estratégico de Tecnologías de Información y Comunicaciones – PETIC, el cual se convierte en la hoja de ruta de innovación de la gestión de TIC y orienta las decisiones ante la dinámica de la industria, de la normatividad y los procesos.
- Implementación de nuevas capacidades y/o servicios como son la solución para automatización de copias de respaldo, la solución de almacenamiento y el avance en la evolución de los sistemas de información (SEA, SI-UPRA).
- Fortalecimiento del equipo de trabajo en la línea de Estrategia TIC y Gestión de Proyectos TIC.
- Avances en la sensibilización y apropiación del Marco de Referencia de Arquitectura Empresarial para la gestión TIC, según lo establecido en el Decreto 2573 de 2014. Dicho

“Marco de Referencia es el instrumento principal y la carta de navegación para implementar la Arquitectura TI en la Entidades Públicas.

- Avances en la implementación de la Estrategia de Gobierno en línea, en la cual la Entidad fue reconocida por el Ministerio TIC y otorgó a la UPRA el premio EXCEL GEL como “Dinamizador del Ecosistema Digital” por su gestión en la implementación de buenas prácticas de TI, apropiación de lineamientos GEL en la Unidad y en el sector de agricultura.
- Fortalecimiento de la infraestructura de soporte a los servicios tecnológicos, mediante la adquisición de capacidades TIC, tales como: Licencias de software (Licencias de ArcGIS for Desktop Basic Concurrent License, actualización de Basic a ArcGIS for Desktop Advanced, (3) Licencias de la extensión ArcGIS Spatial Analyst, Licencia de la extensión ArcGIS Geostatistical Analyst, Licencia ArcGIS for Server Enterprise, Licencia de SAS para servidor, Licencias de sistema Operativo Windows server data center edition) y Hardware de productividad (11 Equipos de cómputo de escritorio, 3 impresoras, (1) Escáner, (20) Diademas de comunicación).
- Avance durante la vigencia 2015 en la puesta en marcha del Sistema de Seguridad de la Información. Durante dicha vigencia se desarrollaron e implementaron las fases de “Planear” y “Hacer” del ciclo PHVA en la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, de conformidad con los estándares establecidos bajo la norma técnica colombiana NTC-ISO IEC 27001 y en cumpliendo con los lineamientos establecidos en el Manual de Gobierno en Línea (GEL).
- Se integró el Sistema de Gestión de Seguridad de la Información - SGSI al Sistema de Gestión Integral – SGI. Sobre el particular se definió el manual, la política y los objetivos de seguridad de la información; adicionalmente se creó la metodología de valoración de riesgos asociados a los activos de información, articulada con la metodología que se implementa actualmente a los riesgos de calidad y de corrupción.
- Por último, se realizó el levantamiento de los activos de información, en el cual se valoró la confidencialidad, integridad y disponibilidad, para determinar su criticidad y de esta manera realizar el análisis de riesgos a los cuales se encuentran expuestos, e identificar los controles a implementar con el fin de mitigar los riesgos identificados. Esta herramienta es de vital importancia para el fortalecimiento del Sistema de Seguridad de la Información de la UPRA

Por otro lado evidenciamos oportunidades de mejora en temas relacionados con la Gestión de Infraestructura, Gestión de Sistemas de Información y Gestión de Proyectos, los cuales se desarrollarán en el cuerpo del informe.

V. Riesgos y Controles

V.I. Riesgos Adicionales

Esta auditoria logró identificar riesgos adicionales que no se encuentran identificados y documentados en la “*Matriz de Riesgos Institucional del Proceso de Gestión de la Información y el Conocimiento*”, y que hacen parte de la cadena de valor del mismo.

Por lo anterior se recomienda evaluar la matriz adjunta al presente informe y calificar la pertinencia de incluirlos dentro del Mapa de Riesgos Institucional. Los riesgos identificados corresponden a los siguientes:

- ✓ Incumplimiento en la ejecución de los planes, programas y/o proyectos establecidos en el PETIC.
- ✓ Pérdida de trazabilidad en el control de versiones o control de productos de TI. (En aplicaciones heredadas, desarrolladas o tercerizadas).
- ✓ Ausencia de recursos para la adquisición de servicios de soporte y mantenimiento de los activos críticos de la plataforma TIC

Sobre el particular, es necesario que cada dueño de proceso realice el ejercicio permanente de revisión de sus riesgos, en concordancia a lo establecido en el Manual MECI el cual determina: “*con el fin de garantizar si los existentes, siguen siendo riesgos para la entidad o proceso, o si existen nuevos riesgos no identificados producto de cambios en el interior del proceso o de su entorno*”. Por lo anterior, se debe involucrar en la administración de los riesgos a los servidores públicos, realizando reuniones de trabajo que tengan como fin identificar nuevos riesgos y/o factores de riesgo en las actividades que se ejecutan dentro del proceso o para la entidad en general.

V.II Riesgos Actuales

De otra parte se realizó la revisión a los riesgos del proceso plasmados en el “*Mapa de Riesgos Institucional*” publicado en la web de la Unidad. Al respecto, se evidenciaron algunas oportunidades de mejora que pueden ser tenidas en cuenta para la formulación de próximos riesgos y causas, así:

V.II.I RIESGO 1: Falla en la plataforma tecnológica

CAUSA: Considerar adicionar las siguientes causas, especificando el control respectivo:

- ✓ Falta de implementación de las Políticas de seguridad
- ✓ Ausencia de un Plan de Gestión de capacidad
- ✓ Carencia de procedimientos para la gestión de proveedores.
- ✓ Ausencia de umbrales de procesamiento y almacenamiento de recursos tecnológicos.
- ✓ Ausencia de un Comité de Control de Cambios de Infraestructura.
- ✓ Ausencia de un procedimiento y/o actividad formal para realizar rooll back.
- ✓ Ausencia de ANS de servicios para el soporte y asistencia técnica.
- ✓ Carencia del Plan de Recuperación de Desastres.

- ✓ Carencia del procedimiento de Gestión de la disponibilidad.

1.2 DOCUMENTACIÓN DEL CONTROL: Considerar revisar la documentación y redacción de los siguientes controles:

- ✓ Procedimientos documentados y formalizados con la respectiva aplicación de formatos, se sugiere el siguiente texto: verificar por parte del funcionario xxxx la aplicación del procedimiento xxxx con periodicidad xxx.
- ✓ Plan de mantenimiento de la plataforma tecnológica, se sugiere el siguiente texto: verificar por parte del funcionario xxx la ejecución del plan de mantenimiento xxx con periodicidad xxx.
- ✓ Políticas de seguridad, se sugiere el siguiente texto: supervisar la aplicación de las políticas de seguridad implementadas con periodicidad xxxx.
- ✓ Definición de los niveles de soporte para la prestación de servicios externos, se sugiere el siguiente texto: Verificar y evaluar por parte del supervisor del contrato los ANS establecidos.

Controles adicionales a los establecidos, se sugiere:

- ✓ Verificar la adecuada financiación de los bienes y/o servicios que soportan la operación de la plataforma TIC.
- ✓ Realizar el monitoreo permanente y continuo de la disponibilidad de los servicios establecidos en el Manual de Acuerdos de Niveles de Servicio.

V.II.II RIESGO 2: Soluciones de software no acordes a los requerimientos de los usuarios

2.2 CAUSA: Considerar el adicionar las siguientes causas:

- ✓ Carencia de estándares de programación y arquitectura de software.
- ✓ Ausencia de un comité de control de requerimientos formal que evalué los requerimientos desde el punto de vista, tecnológico, funcional y financiero.
- ✓ Debilidad en la supervisión tecnológica de los desarrollos de software.
- ✓ Ausencia de un procedimiento formal de gestión de desempeño.
- ✓ Ausencia de un procedimiento formal para realizar rooll back.
- ✓ Ausencia de un procedimiento de gestión de versiones del software aplicativo.
- ✓ Ausencia de ANS para el desarrollo de software aplicativo.

2.2 DOCUMENTACIÓN DEL CONTROL: Considerar el revisar la documentación y redacción de los siguientes controles, así:

GIC-PD-004 Ingeniería de software V2
GIC-FT-016 Solicitud de desarrollo V2
GIC-FT-015 Plan de trabajo V1
GIC-FT-014 Matriz de ejecución de pruebas V1
GIC-FT-013 Plan de pruebas V1

GIC-FT-012 Documento de arquitectura
GIC-FT-011 Plan de riesgos
GIC-FT-010 Manual del usuario
GIC-FT-009 Manual de instalación y configuración
GIC-FT-008 Manual de administración base de datos
GIC-FT-007 Documento diseño base de datos
GIC-FT-006 Documento de análisis.
GIC-FT-005 Diccionario de datos

Se sugiere revisar la documentación de los controles establecidos ya que el formato fortalece el ambiente de control pero es necesario la verificación o revisión o aprobación del mismo, se sugiere el siguiente texto: Revisar y aprobar por parte del funcionario xxx la calidad y completitud del documento xxx con periodicidad xxx.

Controles adicionales a los establecidos se sugiere:

- ✓ Realizar la evaluación funcional, tecnológica y financiera de los requerimientos a partir del modelo de gobierno de TIC.
- ✓ Aprobar y actualizar los planes de trabajo por cambios en los requerimientos de la línea base (requerimiento original).

VI. Hallazgos y Oportunidades de Mejora

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
(OM) Debilidades en la Gestión de Servicios Tecnológicos				
1.	<p>En la revisión efectuada al procedimiento de Administración de Infraestructura, se evidenció:</p> <p>a) Se evidencia que existe un Manual de ANS, no obstante no se ha definido un cronograma específico para su implementación acorde a lo definido en el Plan de Acción Institucional en la política de eficiencia Administrativo - Gestión TI vigencia 2016. Así mismo el diseño del procedimiento no incluye Acuerdos de Niveles de Servicio.</p> <p>b) Se viene efectuando la actividad de mantenimiento preventivo de tipo lógico, la cual no se encuentra documentada en el procedimiento GIC-PD-006 Administración de Infraestructura Tecnológica. Así mismo, la presente actividad no se viene registrando en la hoja de vida de los equipos.</p> <p>c) No se han definido umbrales para los activos tecnológicos de infraestructura, con base en los cuales se detecte de forma oportuna el consumo de recursos al límite de capacidad.</p> <p>d) No existe un plan de capacidad que permita gestionar la misma. Lo anterior con el fin de ofrecer servicios de TI que incluya los recursos tecnológicos de infraestructura garantizando la continuidad en la prestación de los servicios.</p> <p>e) Se observa que las actividades relacionadas con gestión de cambio</p>	<p>Riesgo: Fallas en la Plataforma Tecnológica</p> <p>Impacto: Mayor</p> <p>Probabilidad de ocurrencia: Probable</p>	<ul style="list-style-type: none"> Establecer e implementar un Plan operativo para viabilizar la implementación de los Acuerdos de Niveles de Servicio establecidos. Evaluar el costo/beneficio de la implementación del monitoreo de la plataforma tecnológica aplicando herramientas automatizadas. Para lo anterior es importante tener en cuenta alternativas de contratación de este tipo de servicios y/o adquisición de las herramientas. Establecer políticas y procedimientos para la implementación de la Gestión de la capacidad de los servicios tecnológicos que garanticen la continuidad en la prestación de los servicios. 	<p>Responsable:</p> <p>Fecha de Implementación</p>

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	<p>inmersas en el procedimiento GIC-PD-006 Administración de Infraestructura Tecnológica (numerales 30 a 42) no tienen establecidos controles que apunten a mitigar el riesgo de fallas en la plataforma o interrupción de los servicios.</p> <p>f) Lo establecido en el control "5" del procedimiento GIC-PD-006 Administración de Infraestructura Tecnológica "notificar al generador de la solicitud el resultado del análisis de la viabilidad técnica" no es un control, sino una extensión de la actividad de evaluación del requerimiento. Cabe resaltar que la presente evaluación debe dejar evidencia documental de la pertinencia tecnológica y su beneficio/costo.</p> <p>g) No existe un plan documentado y aprobado para la implementación del Dominio Servicios Tecnológicos, el cual se encuentra establecido en el Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de Información. Cabe resaltar que la fecha límite para cumplir con el 100% es el 2018 de acuerdo a lo establecido en el Decreto 2573 del 12 de diciembre de 2014. Sin embargo, el mismo Decreto establece metas parciales del 25% y del 50% para el 2015 y 2016 respectivamente. Cabe resaltar que la Unidad reporto el avance en la implementación del Decreto pero a la fecha no se ha tenido respuesta</p>		<ul style="list-style-type: none"> Fortalecer la Gestión de Cambios de la plataforma tecnológica mediante la creación de políticas y procedimientos orientados a la mitigación del riesgo de interrupción de los servicios TI. Ajustar el procedimiento GIC-PD-006 Administración de Infraestructura Tecnológica en lo que corresponde a dejar evidencia y ejercer control sobre los requerimientos especiales. Definir, documentar, aprobar y ejecutar un plan para el fortalecimiento del Dominio Servicios Tecnológicos el cual se encuentra establecido en el Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías Información. Fortalecer el modelo de gestión 	

