Unidad de Planificación Rural Agropecuaria

Radicado No. 20165100079 Fecha 31-05-2016 Hora 18:59:47
Proceso: 1034 Anexos: 0 Tipo: Folios: 10 Radicado Por: Claudia Guerrero Tavera
Remitente: Camilo AndrésPulido Laverde
Asunto: Informe Final Auditoria Proceso Gestión de Información y Conocimiento.
Destinatario: Daniel Mauricio Rozo Garzón
Area: Oficina TIC

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

upra
Unidad de Planificación
Rural Agropecuaria

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Contenido

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

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

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

"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, actualization 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.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

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.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

- ✓ 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 implementas 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

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

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).

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

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.	En la revisión efectuada al procedimiento de Administración de Infraestructura, se evidenció: 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. 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. 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. 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. e) Se observa que las actividades relacionadas con gestión de cambio	**Riesgo:** Fallas en la Plataforma Tecnológica **Impacto:** Mayor **Probabilidad de ocurrencia:** Probable	• 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.	**Responsable:** **Fecha de Implementación**

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	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. 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. 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		• 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	

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	por parte del Min.Tic y el Dafp. h) La aplicación del control, de monitoreo de la plataforma tecnológica registra una frecuencia semanal, lo cual no es suficiente para detectar de forma preventiva y oportuna los eventos que requieran intervención de mantenimientos preventivos y/o correctivos. i) La Unidad no ha conformado una instancia de Gobierno de los Cambios en la Plataforma Tecnológica, el cual tenga como mínimo la función principal de la evaluación del riesgo, evaluación tecnológica y evaluación de impacto de los cambios requeridos en la plataforma, ya sea de tipo correctivo, preventivo o evolutivo. j) El procedimiento de Administración de Infraestructura carece de un documento de Políticas de Gobierno y Gestión de los recursos de infraestructura. Cabe aclarar que el Manual de Políticas de Seguridad de Información es una parte pero no el todo del conjunto de las políticas para la Gestión. Cabe resaltar que una adecuada armonización al dominio de servicios tecnológicos permitirá gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en la entidad.		y gobierno de los recursos de infraestructura mediante la definición de Políticas de Gobierno y Gestión de los recursos de infraestructura. • Todo proyecto que surja de la gestión de infraestructura requiere su inclusión y actualización en el PETIC.	

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

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 Copias de Seguridad				
2	En la revisión efectuada al procedimiento de Copias de Seguridad, se evidenció: a) No se ha documentado, formalizado y socializado las Políticas de copias de respaldo de la Información. b) Desactualización respecto de las actividades que se realizan dada la implementación de la solución automatizada Backup Exe Veritas. c) No se tienen formalmente definidos la ejecución de las copias de respaldo de la información contenida en los Motores de Bases de Datos Relacionales – RDBMS. Adicionalmente se observa que el gobierno y control sobre esta actividad está disperso en diferentes áreas. (Sistemas de información, Administración de Infraestructura y Usuarios finales) d) No se tienen establecidas actividades de pruebas de conformidad tecnológicas de las copias de seguridad. Carencia que incrementa la probabilidad de perdida de información. Cabe aclarar que pese a lo observado, la entidad para la vigencia 2016 ha venido ejecutando y obteniendo copias de respaldo de la información, ubicada en las unidades de red U y Z, las bases de datos (SQLServer, Postgres y Oracle) y de las máquinas virtuales.	**Riesgo:** Fallas en la Plataforma Tecnológica **Impacto:** Mayor **Probabilidad de ocurrencia:** Posible	• Fortalecer las políticas y procedimientos referentes al tema de copias de respaldo, mediante la actualización del procedimiento teniendo como referente la solución automatizada, las políticas establecidas en el Manual de Políticas de Seguridad de Información de la Entidad y lo establecido para este tema en el Dominio Servicios Tecnológicos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. • Ampliar el alcance de las políticas y procedimientos de las copias de respaldo incluyendo la información contenida en los Motores de Bases de Datos Relacionales que soportan los sistemas de información de la	**Responsable:** **Fecha de Implementación**

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	Se resalta que la información es uno de los activos más importantes para la entidad y los funcionarios que trabajan en ella, por lo tanto, realizar respaldos periódicos es una tarea que debe considerarse prioritaria y en ningún caso hay que subestimar las múltiples causas por las que podría ocurrir una situación de pérdida de información. Por lo anterior, realizar este procedimiento de la forma adecuada, es decir, considerando la información a resguardar, los tipos de backup existentes, los medios de almacenamiento, la frecuencia de respaldo y la custodia; resulta primordial para proteger correctamente la información.		Entidad. • Establecer actividades de pruebas de conformidad tecnológica de las copias de respaldo. • Establecer los roles y responsabilidades de cada uno de los actores involucrados en la gestión de copias de respaldo de la información corporativa de la Entidad.	
(OM) Debilidades en la Gestión del Soporte y Asistencia Técnica				
3	En la revisión efectuada al procedimiento de soporte y asistencia técnica, se evidenció: a) El control "Verificar in situ el nivel de complejidad de la solicitud", no tiene definidos registros que permitan tener evidencia de su aplicación y posterior evaluación. Por lo anterior el control no es efectivo y debe ser revisada su definición. b) El procedimiento carece de actividades y registro para el diagnóstico, plan de atención y solución y evaluación del servicio, con base en los cuales el procedimiento de soporte pueda ser gestionado y controlado. c) El procedimiento no cuenta con niveles de escalamiento tanto a nivel de otras áreas de la oficina TIC como a los proveedores de bienes y/o servicios TIC, en los	**Riesgo:** Fallas en la Plataforma Tecnológica **Impacto:** Posible **Probabilidad de ocurrencia:** Probable	• Ajustar el procedimiento en su definición del alcance para que cubra la totalidad de los posibles servicios de soporte y asistencia técnica. • Fortalecer el procedimiento incluyendo actividades y registros para el diagnóstico, plan de atención y solución, evaluación del servicio. • Fortalecer el procedimiento incluyendo	Responsable: Fecha de Implementación

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	casos que el primer nivel no esté en capacidad de atender la solicitud. d) El procedimiento no cuenta con la definición formal y evaluación de Acuerdos de Niveles de Servicio, los cuales permitirían tener claridad al usuario de las características del mismo. Cabe resaltar que para lograr mejores niveles de servicio y eficiencia en el servicio de soporte y asistencia técnica la industria de TI ha venido implementado modelos de mesa de servicio ya sea tercerizada o con recursos internos de las organizaciones. Estas mesas de servicio están gestionados con base en buenas prácticas de la industria como lo es ITIL-Information Technology Infrastructure Library. Adicionalmente no se debe entender que implementar un modelo de mesa de servicio es únicamente implementar una herramienta de software especializada para este tema, involucra adicionalmente implementar procesos, buenas prácticas de gestión TI y cultura de servicio al cliente. Finalmente, la función de la Mesa de Ayuda provee a los usuarios un punto único de contacto mediante el cual se resuelvan y/o canalicen sus necesidades relativas al uso de recursos y servicios de plataformas tecnológicas, su implementación busca como beneficios principales: Atender todas los requerimientos, solicitudes, incidentes recibidos, resolver un alto porcentaje en el primer nivel, tener adecuado seguimiento de cada caso, responder de manera oportuna, eficiente y con adecuada calidad, incrementar la productividad de la entidad, proveer información para el mejoramiento continuo y mejorar los niveles de disponibilidad de los servicios tecnológicos.		actividades de escalamiento de la solicitud tanto a nivel de áreas de la oficina TIC como a los proveedores de bienes y/o servicios TIC. • Definir e implementar Acuerdos de Niveles de Servicio y fortalecer el procedimiento incluyendo actividades para el seguimiento y control de los mismos. • Evaluar la prioridad de la implementación de un modelo de Mesa de Servicio para la atención de los requerimientos, incidentes y problemas presentados en los bienes y servicios basados en TIC de la Entidad, lo anterior debe permitir la gestión eficiente de este servicio y mejorar el nivel de satisfacción de los usuarios.	

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

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 Sistemas de Información				
4	En la revisión efectuada al procedimiento de Ingeniería de Software, se evidenció: a) El objetivo y alcance del procedimiento no se encuentra adecuadamente definido y armonizado con el Marco de Referencia, lo anterior dado que se encuentra limitado en su alcance, al referir únicamente a la gestión del ciclo de vida del software. Sobre el particular se deja de lado otros elementos fundamentales para la gestión de los sistemas de Información como lo son la planeación y gestión, el diseño, el ciclo de vida, el soporte y la gestión de la calidad y seguridad de los mismos. b) El procedimiento no clasifica los requerimientos entre productos en producción y/o de nuevas soluciones. La importancia de dicha tipificación radica en la gran diferencia en esfuerzo e impacto de cada uno de estos tipos de requerimientos. c) La Actividad 3 "Informar al solicitante mediante correo electrónico el resultado de la evaluación de su solicitud y las acciones a seguir" y en la Actividad 4 "Informar al solicitante mediante correo electrónico si la solución se desarrollará de forma interna/externa y las acciones a seguir", no son controles si no corresponden a situaciones que extienden la actividad principal.	**Riesgo:** Soluciones de software no acordes a los requerimientos de los usuarios **Impacto** Moderado **Probabilidad de ocurrencia** Probable	• Fortalecer y armonizar el Sistema de Gestión Integral del Proceso de Gestión de Información y Conocimiento para el área de Sistemas de Información teniendo como modelo el Dominio de Sistemas de Información establecido en el Marco de Referencia de Arquitectura de TI. • Tomar las medidas necesarias para ejercer gobierno y control sobre el 100% de los sistemas de información que soportan los procesos de apoyo, misionales, estratégicos y de evaluación de la Entidad. • Establecer formalmente las responsabilidades y actividades del rol del líder funcional o administrador funcional del o los sistemas de información en operación.	

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	d) La justificación de las evaluaciones realizadas a los requerimientos presentados por el usuario no involucran aspectos mínimos de viabilidad funcional, viabilidad tecnológica y viabilidad financiera. Cabe resaltar que la completitud de la evaluación permite dejar evidencia razonable y de forma clara la situación presentada para las partes interesadas. Es claro que cada requerimiento involucra inversión de recursos a todo nivel (tiempo, humanos, financieros), por lo tanto la evaluación debe ser consistente y alineada con los objetivos de la Entidad. e) El procedimiento solo involucra a los funcionarios del área de TIC para tomar la decisión de aceptar o rechazar los requerimientos. Lo anterior no permite tener una separación de roles de la Gestión de los requerimientos y/o necesidades de los usuarios finales. Cabe resaltar que para una efectiva planeación y priorización de requerimientos de sistemas de información es necesario que se involucren otros roles y funcionarios de la Entidad y se establezca un modelo formal de Gobierno de los mismos. f) El procedimiento no establece actividades y/o controles para la gestión de versiones del software al igual que no se tienen establecidas políticas para el versionamiento de cada una de las aplicaciones que tienen desarrollo a la medida. Cabe resaltar que la Gestión de Versiones tiene los siguientes		• Tomar las medidas necesarias para que se dé estricto cumplimiento en la aplicación eficiente de los controles referentes con las actividades de aprobación y verificación de documentos y/o entregables que forman parte de los artefactos de los sistemas de información. • Documentar y o ajustar el modelo de gobierno para la gestión de requerimientos de mantenimiento o adquisición de sistemas de información. Dicho modelo debe asegurar la alineación de cada requerimiento con la estrategia de la Entidad, asegurar su viabilidad financiera, tecnológica y funcional como también la priorización de los mismos. Este modelo debe tener en cuenta la participación de los dueños de proceso involucrados en las iniciativas de automatización.	

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	objetivos: Establecer una política de implementación de nuevas versiones del software, implementar las nuevas versiones de software en el entorno de producción tras su verificación en un entorno realista de pruebas, garantizar que el proceso de cambio cumpla las especificaciones, alinear esta actividad con la gestión de cambios, organizar copias idénticas del software en producción, así como de toda su documentación asociada. Lo anterior permitirá mitigar el riesgo de deterioro de la calidad de los sistemas de información. g) El procedimiento carece de definición y especificación en temas de seguridad, privacidad y trazabilidad para los sistemas de información. Cabe resaltar que es requisito fundamental de las soluciones el contar con capacidades que aseguren la información y permitan como mínimo el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios de los sistemas de información, mitigar el riesgo de acceso no autorizado y la integralidad de la información. h) El área de Sistemas de Información no tiene gobierno en lo que le compete al Sistema de Información SIGEP. El tener gobierno y control del 100% de las aplicaciones que soportan los procesos de la Entidad asegura unidad de criterio y gestión sobre este tipo de recursos. Adicionalmente mitiga el riesgo de atomizar la gestión sobre los			

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	mismos. i) No se cuenta con segregación de roles para la gestión de las etapas básicas del ciclo de vida del software. La separación de roles se hace más relevante, teniendo en cuenta que la Unidad hace construcción de software con recursos internos. Los roles principales de Analista de Requerimientos, Desarrolladores de Software, Arquitecto de Software y Calidad permiten tener un esquema de soporte para el aseguramiento de la calidad de los productos de software. j) Se observaron inconsistencias, desactualizaciones, falta de revisión, aprobación y completitud en el diligenciamiento de los formatos establecidos en el procedimiento y que hacen parte de la evidencia de la aplicabilidad de los controles del mismo, así: ✓ Formato GIC-FT-006 Documento de Análisis de Requerimientos - Requerimiento Indicadores. La inconsistencia se refleja en que la fecha de creación del documento y el número de versión se diligencian con datos diferentes dentro del mismo documento. ✓ En el Plan de trabajo GIC-GT-015 no se tienen en cuenta actividades para la puesta en marcha de las soluciones de software las cuales hacer parte de la fase de transición. ✓ Documento GIC-FT-010			

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	Manual del Usuario SIPRA no se encuentra actualizado con respecto al alcance y la versión vigente puesta en producción en abril 8 de 2016. De igual forma no se evidencia cumplimiento de la revisión y aprobación del documento. ✓ Documento GIC_FT-007 Diseño de Base de Datos Indicadores: presenta inconsistencias en su elaboración, teniendo en cuenta que la fecha de creación presenta una fecha anterior a la fecha de aprobación del requerimiento, lo cual no es lógico de acuerdo con la secuencia de actividades del procedimiento. Adicionalmente la evidencia de la aprobación del documento presenta inconsistencia ya que se realiza en enero de 2016, lo cual no es coherente con la secuencia lógica del procedimiento. ✓ Documento GIC-FT-005 Diccionario de Datos Módulo de indicadores SIUPRA: se encuentra desactualizado y presenta inconsistencias con respecto a la solución implementada en producción. Lo anterior genera riesgos de obsolescencia de los artefactos que conforman el producto de software generando riesgo de inviabilidad del			

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	mantenimiento del software k) El procedimiento carece de actividades y formatos para registrar la trazabilidad de la ejecución de los escenarios de pruebas establecidos en el plan para el efecto. La evidencia de ejecución de las pruebas hacen parte del aseguramiento de calidad del producto y permite mitigar el riesgo de no conformidades del producto. l) El procedimiento carece de actividades de pruebas de aceptación por parte de los usuarios funcionales o quien haga sus veces. Las pruebas de aceptación son una actividad fundamental para el aseguramiento de calidad de los productos de software y son igualmente importantes en la apropiación del producto. Para eliminar la influencia de conflictos de intereses, y para que sea lo más objetiva posible, la prueba de aceptación nunca debería ser responsabilidad de los ingenieros de software que han participado en la construcción del producto. m) El procedimiento carece de la definición e implementación de Acuerdos de Niveles de Servicio para el Soporte de los Sistemas de Información. Cabe resaltar que el elemento de soporte y los ANS permiten organizar los lineamientos y guías para identificar y considerar aspectos requeridos en los procedimientos relativos a la gestión de solicitudes de cambio sobre los Sistemas de Información de la Entidad, que pueden ser originadas por nuevos requerimientos, cambios del			

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	entorno o fallas detectadas en los componentes del software.			
OM: Debilidades en la Gestión de proyectos				
5	a. Los proyectos ejecutados en el año 2015 carecen de la documentación mínima para evaluar el cumplimiento de lo presupuestado vs. lo ejecutado a nivel de las variables de alcance, tiempo, presupuesto y calidad. Lo anterior evidencia debilidades en la gestión de proyectos apoyados en metodologías comúnmente aceptadas. b. Durante los primeros cinco (5) meses del año 2016 no hay evidencia formal de metodología de proyectos de avance en la ejecución de los proyectos planteados en el PETIC. Una vez verificada la situación con los líderes de Estrategia y Gobierno, se informó que el mismo se encuentra en revisión en cuanto al alcance y priorización. Adicionalmente se informa que la nueva versión del plan de proyectos se oficializará a mediados del año. Lo anterior, evidencia que se carece de evidencias de seguimiento que permitan evaluar el estado y avance de los proyectos. c. La Unidad carece de una metodología de gestión de proyectos formal dentro del Sistema de Gestión Integral. Lo anterior incrementa la probabilidad de que se materialice el riesgo de incumplimiento de planes, programas y proyectos. Se resalta que de acuerdo con lo establecido en el Marco de Referencia de	**Riesgo:** Incumplimiento del plan de proyectos **Impacto** Mayor **Probabilidad de ocurrencia** Probable	• Fortalecer el Proceso de Gestión de Información y Conocimiento con Políticas, Procedimientos y Controles para la adecuada Gestión de Proyectos. Para el diseño de lo anterior se debe tener cuenta como mínimo lo establecido en el Marco de Referencia de Arquitectura Empresarial para Gestión de TI. La Gestión Integral de proyectos, busca la adecuada gestión de programas y proyectos asociados a TI, incluye el direccionamiento de proyectos de TI y el seguimiento y evaluación de los mismos. • Los recursos humanos que lideran y/o participan en los proyectos no deben compartir actividades o	

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Nº	Hallazgos (H) y/o Oportunidades de Mejora (OM) y/o (O) Observación	Riesgo, Impacto, Categoría	Recomendación	Plan de acción
	Arquitectura Empresarial para Gestión de TI, la Gestión Integral de proyectos, busca la adecuada gestión de programas y proyectos asociados a TI. Así mismo, incluye el direccionamiento de proyectos de TI y el seguimiento y evaluación de los mismos. d. Los recursos humanos que lideran y/o participan en los proyectos comparten actividades o responsabilidades en la operación de la Unidad. Lo anterior genera riesgo de incumplimiento de los planes de los proyectos. Cabe resaltar que existen múltiples beneficios de la implementación de un modelo de gestión de proyectos, entre los cuales están: Eficiencia en la entrega de los proyectos, aumenta la satisfacción de los clientes, aprendizaje y aprovechamiento de la experiencia, mejora la unión y el desarrollo del equipo, mayor ventaja competitiva, mayor control de los riesgos de los proyectos, aumento de la calidad y aumento de la Cantidad, por lo anterior es importante fortalecer el ambiente de control para la gestión de proyectos.		responsabilidades con la operación de la Entidad de forma paralela. Lo anterior teniendo en cuenta que esta situación es una de las causas de incumplimiento de los planes de los proyectos. • Tomar las medidas pertinentes para que las revisiones a los proyectos del PETIC sean realizadas de forma oportuna y antes del inicio de la vigencia presupuestal.	