Contenido

I. Objetivo

Realizar una auditoría a las actividades desarrolladas por el procedimiento de Ingeniería de software en la UPRA, aplicando buenas prácticas para el desarrollo de software con el fin de generar un diagnóstico y recomendaciones.

II. Alcance

Proceso Gestión de Información y Conocimiento: Procedimiento Ingeniería de software GIC-PD-004, riesgos identificados para el proceso y relacionados con el procedimiento de Ingeniería de Software, cumplimiento de políticas del sistema de gestión institucional, guía metodológica para el desarrollo de software, y proyectos desarrollados o en desarrollo vigencia 2018 y 2019.

III. Criterios de Auditoria

- Procedimiento de Ingeniería de Software (GIC-PD-004 versión 6 del 17/05/2018).

En los procesos de Direccionamiento Estratégico, a partir de los cuales se definen los programas, proyectos, planes, estrategias, objetivos, provisión de la comunicación, aseguramiento de recursos y revisiones por la dirección, se incluye el proceso de Gestión de Información y Conocimiento (GIC-PR-001) al cual pertenece el procedimiento de Ingeniera de Software.

La verificación realizada a este procedimiento tiene como finalidad la revisión de sus actividades con el objeto de establecer si cuentan con una estructura sistemática de trabajo, que permita el cumplimiento del objetivo del procedimiento y su aplicabilidad permite atender las exigencias de la calidad requeridas para satisfacer los requerimientos de las partes interesadas. Además, de dar cumplimiento al Instructivo de elaboración de documentos del Sistema de Gestión Integrado y a los formatos asociados, establecidos en dichos documentos.

- Cumplimiento de políticas del Sistema de Gestión Institucional.

De acuerdo con la guía Código de Buen Gobierno (PLE-GU-001 versión 4 del 14/12/2018) en su numeral 3.6.11. Políticas de Operación, se verifica mediante el procedimiento de Ingeniería de Software y la ejecución de sus actividades, el cumplimiento de la política para el Direccionamiento Estratégico relacionada con: "La UPRA establecerá estándares para el manejo de sus conjuntos de datos, en los dominios de información, de análisis de información y de sistemas de información en desarrollo de los procesos institucionales".

- Matriz de Riesgos (GIC-RI-001 versión 3 del 1/31/2018)

Tomando como base los riesgos institucionales y de corrupción identificados para el proceso de Gestión de Información y Conocimiento, relacionados directamente con el Procedimiento Ingeniería de software GIC-PD-004, se verificará su identificación, valoración y las acciones para su control y tratamiento.

- Modelo CMMI para el desarrollo de software.

Teniendo en cuenta los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), en su guía G.SIS.01 Guía del dominio de Sistemas de Información, en cuanto al lineamiento LI.SIS.05 Metodología de referencia para el desarrollo de sistemas de información; se consideró en la planeación de la presente auditoria y como parámetro de validación para el proceso de desarrollo de software, la utilización de los lineamientos dados por la metodología CMMI (Capability Maturity Model Integration); sin embargo, la oficina TIC de la UPRA definió una metodología formal para el desarrollo y mantenimiento de software, tomando como base las buenas prácticas de Scrum y Kanban, la cual orienta los proyectos de construcción o evolución de los sistemas de información que se desarrollen a la medida.

En tal sentido, la evaluación de la metodología aplicada para el desarrollo de software se fundamentó en los lineamientos adoptados por la UPRA en su Guía Metodológica de Referencia de Sistemas de Información (GIC-GU-006 versión 2 del 01/08/2018).

- Proyectos vigencia 2018 y 2019.

Con el objeto de validar la aplicación de los lineamientos dados en la Guía Metodológica de Referencia de Sistemas de Información (GIC-GU-006 versión 2 del 01/08/2018) se revisaron dos proyectos: Proyecto SIPRA - Sistema de información para la planificación rural agropecuaria (vigencia 2018) y Proyecto SIGRA - sistema de información para la gestión de riesgos agropecuarios (vigencia 2019).

IV. *Procedimientos Adelantados*

El presente informe contiene las actividades de verificación que se desarrollaron tomando como base la documentación del proceso de Gestión de Información y Conocimiento en cuanto al procedimiento de Ingeniería de Software, los lineamientos del procedimiento de auditorías internas de la UPRA, las normas ISO 19011 e ISO 27001, cumplimiento de políticas del Sistema de Gestión Institucional y la Guía Metodológica de Referencia de Sistemas de Información.

Entre las fuentes consultadas se encuentra el Sistema Integrado de Gestión publicado en él aplicativo SEA. La documentación y soportes del procedimiento de Ingeniería de Software solicitados a la dependencia evaluada, en relación con el procedimiento que se sigue en la actualidad, la ejecución de dicho procedimiento y la mejora continua que se les está realizando al mismo.

A continuación, se indican las actividades de auditoría desarrolladas durante la evaluación al proceso de Gestión de Información y Conocimiento en cuanto al procedimiento de Ingeniería de Software:

- Revisión de las actividades indicadas en el procedimiento que se sigue para llevar a cabo la Ingeniería de Software, desde el punto de vista de su planeación, ejecución, control y seguimiento.
- Revisión conceptual de la Guía Metodológica para la implementación exitosa de los sistemas de información nuevos o para el mantenimiento de los existentes, y que ha sido generada y adoptada por la UPRA.
- Revisión de los riesgos y aplicabilidad de los controles que fueron identificados para el procedimiento de Ingeniería de Software
- Revisión de dos proyectos de TIC con el objeto de establecer el nivel de cumplimiento de los procedimientos, generación de registros, seguimiento y control establecidos en el marco del procedimiento de Ingeniería de Software
- Consulta de la información del procedimiento de Ingeniería de Software y del desarrollo de sus actividades o proyectos, publicada en el sitio web de la Entidad y del Sistema de Eficiencia Administrativa (SEA).
- Validación del proceso de mejora continua que se viene ejecutando para el procedimiento de Ingeniería de Software.
- Validación de los aspectos que pueden generar impactos negativos en el normal desarrollo del procedimiento de Ingeniería de Software con el objeto de dictar cursos de mejoramiento y/o actualización de acuerdo con las buenas prácticas internacionales que se tienen al respecto.

V. Principales Riesgos asociados al proceso

- No disponibilidad de la plataforma tecnológica requerida para la prestación de servicios tecnológicos de la UPRA, incluidos en el catálogo de servicios de TI.
- Soluciones de software no acordes a los requerimientos de los usuarios.
- Pérdida de la confidencialidad, disponibilidad e integridad de los activos de información de la UPRA.

VI. Conclusiones

La presente auditoria se realizó basada en el proceso de Gestión de Información y Conocimiento en cuanto al procedimiento de Ingeniería de Software, los lineamientos del procedimiento de auditorías internas de la UPRA, cumplimiento de políticas del Sistema de Gestión Institucional, y se centró en los aspectos/riesgos significativos.

Tomando como base los resultados consignados en el numeral VI del presente informe y de acuerdo con el alcance de la auditoria y el muestreo realizado, se considera que el procedimiento de Ingeniería de Software viene siendo mejorado para lograr un buen nivel de gestión y control y así alcanzar los objetivos del mismo y la atención de los requerimientos en relación con el desarrollo, cambios y gestión de incidentes en los sistemas de información de acuerdo a las necesidades y prioridades de la UPRA.

En relación con los riesgos identificados para el proceso de Gestión de Información y Conocimiento (GIC-PR-001), y que están relacionados directamente con el procedimiento de Ingeniera de Software, consideramos que estos han sido gestionados dando cumplimiento a los lineamentos establecidos en la metodología de riesgos.

Aun así, se generaron algunos lineamientos de control y gestión de actividades y de riesgos que si bien a la fecha no ocasionan desviaciones en la ejecución del procedimiento auditado si pueden llegar a generar hallazgos significativos en un futuro cercano. En todo caso, estos lineamientos permiten el fortalecimiento de las políticas, que regulan la materia y la gestión de los riesgos asociados al proceso, haciendo énfasis en aquellos que pueden comprometer la adecuada gestión de los recursos institucionales.

VII. Observaciones y oportunidades de mejora

Con el radicado 2019-3-002630 se remitió la respuesta al informe preliminar el 5 de agosto de 2019, se realizó reunión el 6 de agosto entre el auditor líder, Juan José Ballesteros de la oficina TICS y Sandra Monroy de la Asesoría de Planeación con el fin de ampliar la descripción de las observaciones encontradas y las oportunidades de mejora teniendo en cuenta los comentarios realizados por TICS. Producto de lo anterior las observaciones se mantienen y se consideró unificar algunas de las oportunidades de mejora para facilitar su implementación.

El resultado del ejercicio de auditoría se presenta a continuación:

N°	Observaciones	Recomendación
	Del Procedimiento Actual de Ingeniería de Software (GIC-PD-004 versión 6 del 17/05/2018)	
1	En el procedimiento no se observan directrices que den las pautas iniciales que permitan orientar a los usuarios en la presentación de sus requerimientos, de acuerdo a la orientación metodológica que se tiene para la implementación de los sistemas de información nuevos o para el mantenimiento de los existentes. Lo anterior, sugiere una observación frente al Numeral 7.5.1. Control de la producción y de la prestación del servicio, toda vez que se dificulta la planificación y realización de los productos bajo condiciones controladas.	Se deben incluir directrices o Políticas que orienten a los usuarios en la presentación de sus requerimientos.
	De la Guía Metodológica de Referencia de Sistemas de Información (GIC-GU-006 versión 2 del 01/08/2018)	
	En cuanto a lo sugerido en el numeral 4. METODOLOGÍA DE REFERENCIA PARA EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN DE LA UPRA, observamos lo siguiente:	
2	No se incluye los aspectos a tener en cuenta para que el Comité CIGD defina la prioridad de atención que se le debe dar a los requerimientos o proyectos que se autorizan y que llegan al equipo de Ingeniería de Software; esto con el objeto de poder programar dichos desarrollos y así dar mejor cumplimiento a la política de operación relacionada con los estándares para el manejo de sistemas de información en desarrollo de los procesos institucionales.	Es necesario establecer los niveles de priorización que se le deben asignar a los diferentes requerimientos o proyectos, teniendo en cuenta su impacto, importancia o relevancia; esto con el objeto de que el equipo de Ingeniería de Software los programe y lleve a cabo su tención de acuerdo a la prioridad establecida.
3	No se observa en la Guía, que haga referencia a la definición de responsabilidades que tiene a cargo el Usuario Solicitante del requerimiento, quien debe actuar como Dueño del Producto siendo responsable de la Lista de requerimientos específicos; lo cual indica que no se consideró lo sugerido al respecto en la metodología Scrum.	Se debe incluir en esta guía o en un documento de Políticas de Sistemas de Información las responsabilidades del Usuario solicitante frente al requerimiento realizado, dichas responsabilidades deben ir relacionadas con: responder oportunamente los mensajes de correo relacionados con el requerimiento, ejecutar plan de pruebas oportunamente, y demás actividades que permitan el normal desarrollo del procedimiento.
4	Si bien se han establecido como puntos de control el generar los requerimientos documentados en el Formato GIC-FT-006 DOCUMENTO DE ANÁLISIS DE HISTORIAS DE USUARIO, y mediante el	Es necesario incluir en el acta de reunión la aprobación, por parte del usuario solicitante, de los criterios de

	Acta de Reunión PLE-FT-003 en la cual se registra la Validación y entendimiento de requerimientos con el usuario solicitante y con desarrollador, no se observa que se tenga la aprobación por parte del usuario solicitante de los criterios de aceptación establecidos para el desarrollo, lo cual sugiere la aprobación del entendimiento de artefactos de la metodología Scrum.	aceptación que se encuentran en el plan de pruebas.
5	En el Numeral 4.1.4 Etapa de pruebas indica que "Todas aquellas actividades que se deben tener en cuenta para la etapa de pruebas, están descritas en el GIC-PD-004 PROCEDIMIENTO DE INGENIERÍA DE SOFTWARE". Sin embargo, en dicho procedimiento se hace referencia a actividades como: Elaborar/Modificar Plan de Pruebas, Elaborar o modificar el formato GIC-FT-013 Plan de Pruebas, Verificar que el o los elementos del Plan de Pruebas se encuentren en el formato, Verificar que el Formato GIC-FT-013 Plan de pruebas se encuentre validado; pero no se hace referencia al as responsabilidades desde el punto de vista de usuario final.	Es necesario incluir en el documento Plan de Pruebas frente a esta Etapa de pruebas las responsabilidades de planeación, ejecución, seguimiento y control de pruebas por parte del usuario final.
	De los Proyectos Auditados: • **Proyecto SIPRA - Sistema de información para la planificación rural agropecuaria (2018)** • **Proyecto SIGRA - sistema de información para la gestión de riesgos agropecuarios(2019).**	
6	Para el proyecto SIPRA se observa el documento de análisis de requerimientos_1.0. (GIC-FT-006) que incluye los aspectos generales de la necesidad a cubrir. Además, se generaron los riesgos del proyecto (Mapa de Riesgos, archivo Excel 20181214_ MRGIC2018_ TercerCuarimestre_TIC), pero no se observa el seguimiento y actualización de los mismos durante la ejecución del proyecto, como está indicado en el Manual del Sistema de Gestión Integrado numeral 6.1. Acciones para abordar riesgos y oportunidades.	En el marco de la Gestión de Proyectos, para los riesgos que se identifiquen, se deben revisar, evaluar, controlar y establecer su estado en cada avance del proyecto según el seguimiento establecido. Esto de acuerdo con la Metodología de riesgos que se ha adoptado en la UPRA.
7	Para los dos proyectos se observa que, si bien se tiene documentos que sugieren la ejecución de diferentes actividades, y que están contempladas en el procedimiento de Ingeniería de Software, no se observan las actividades propias de la Etapa Gerencia de proyectos, como se indica en el numeral 4.1.5 de la Guía Metodológica de Referencia de Sistemas de Información (GIC-GU-006 versión 2 del 01/08/2018) y que hace referencia a "Esta etapa es transversal a todo el ciclo de vida"	Es necesario, que la Gestión de Proyectos, se lleve a cabo en cumplimiento de las actividades propias de este rol tal como se indica en la guía metodológica, esta debe ser durante todo el ciclo de vida de tención de los requerimientos de software. Es necesario dejar registro de las actividades realizadas en el entorno de la Gerencia de cada Proyecto.

N°	Oportunidades	Recomendación
	Del Procedimiento Actual de Ingeniería de Software (GIC-PD-004 versión 6 del 17/05/2018)	
1	En el campo de "control" en la descripción de actividades se presenta información sobre verificar un aspecto que se considera como control, pero no se indica qué se debe hacer en caso de un incumplimiento.	Es necesario evaluar si se deben ncluir en cada una de las actividades acciones de control, lo cual sugiere aplicar controles a actividades que no son susceptibles de amenazas en su ejecución. O en su defecto indicar claramente que actividad se debe hacer en caso de incumplimiento del control.
2	En general, el procedimiento presenta gran cantidad de actividades que sugieren la interrelación de las mismas dado los diferentes tipos de solicitud, esto origina el cruce de actividades y la utilización de muchos símbolos de diagramación interrelacionados que no brindan la suficiente claridad para su ejecución y control.	Con el ánimo de lograr un mejor entendimiento y aplicación de los procedimientos, se sugiere la generación de procedimientos por cada tipo de solicitud, como son: desarrollos, cambios en los sistemas e incidencias de sistemas información.
3	El procedimiento presenta actividades que utilizan Compuertas (Gateway) o Control de Flujo (CF), o Compuerta Paralela (CP) las cuales determinan ramificaciones, bifurcaciones, combinaciones y fusiones del proceso, que en nuestro concepto dificultan el entendimiento y por ende, el desarrollo normal del procedimiento.	Llevar a cabo la unificación de aquellas actividades de control de flujo que por su naturaleza lo permitan y se puedan ejecutar en un mismo momento, llevando a que varias actividades confluyan en una misma actividad de control de flujo, utilizando éstas últimas lo menos posible.
	De la Guía Metodológica de Referencia de Sistemas de Información (GIC-GU-006 versión 2 del 01/08/2018)	
4	Según lo indicado en el numeral 1 Objetivo, esta guía tiene como objetivo "dar orientación metodológica para la implementación exitosa de los sistemas de información nuevos o para el mantenimiento de los existentes, por lo anterior, se presenta la forma cómo se deben realizar los ciclos de desarrollo de software y la relación que tienen estos con las fases de la presente metodología".	Es necesario establecer como lineamento del Equipo Directivo y como mecanismo de control una política que indique el obligatorio cumplimiento, a todo nivel, de las fases de la metodología que nos ocupa, lo cual redundará en la implementación exitosa de los sistemas de información y, por ende, al cumplimiento de esta guía metodológica.
	En cuanto a lo sugerido en el numeral 4. METODOLOGÍA DE REFERENCIA PARA EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN DE LA UPRA, observamos lo siguiente:	

5	En el numeral 4.1.2.1.9 Mantenibilidad, hace referencia a la facilidad para el mantenimiento y evolución de un sistema de información, lo cual involucra Corregir errores, Desarrollar nuevos requerimientos del cliente y Adaptarse a cambios ambientales. Para la UPRA el principio de mantenibilidad involucra corregir errores en lo que se pueda diagnosticar las causas de fallo, desarrollar nuevas funcionalidades, adaptarse a cambios que surjan por la normatividad o direccionamientos estratégicos.	Si bien se indica que involucra el concepto de Mantenibilidad al interior de la UPRA, no se hace referencia al cómo se deben desarrollar cada uno de esos aspectos para lograr la Mantenibilidad de los sistemas de información.
6	En el numeral 4.1.2.1.11 Lineamientos de auditoría y trazabilidad de sistemas de información LI.SIS.23, se indica que "Con el objetivo de apoyar a la UPRA en el registro de estos eventos, es indispensable contar con una herramienta correlacionadora de eventos".	Es necesario revisar este párrafo y adecuarlo de forma tal que indique si es una herramienta que se tiene y se debe utilizar o es una necesidad que debe ser cubierta, en tal caso, se debería retirar este párrafo.
	De los Riesgos del Proceso en relación al Procedimiento de Ingeniería de Software	
7	En la Matriz de Riesgos (GIC-RI-001 versión 3 del 1/31/2018) en relación con el procedimiento de Ingeniería de Software se identificaron los riesgos relacionados con Soluciones de software no acordes a los requerimientos de los usuarios. Pero no se observa la inclusión de aquellos riesgos relacionados con la atención de los requerimientos o de ejecución del proyecto y con los riesgos técnicos que se puedan presentar.	Es necesario considerar el incluir en la matriz de riesgos los relacionados con la atención de requerimientos o ejecución del proyecto, como son: el incumplimiento del plan, personal, recursos, cambio de prioridad del proyecto, entre otros. Y desde el punto de vista de riesgos técnicos, se pueden considerar requisitos no claros o cambiantes, deficiencias en el diseño, tiempo de implementación, planeación y ejecución de pruebas, Incertidumbre técnica, tecnologías desconocidas, entre otros.
	De los Proyectos Auditados: • **Proyecto SIPRA - Sistema de información para la planificación rural agropecuaria (2018)** • **Proyecto SIGRA - sistema de información para la gestión de riesgos agropecuarios(2019).**	
8	En general, y de acuerdo a lo observado la planeación y seguimiento de los proyectos se basa en gran medida en la herramienta Excel, lo cual dificulta realizar el seguimiento y control de las actividades de todos los proyectos en curso.	Consideramos procedente estudiar la viabilidad de contar con las actividades propias de la Gerencia de Proyectos apoyadas en una herramienta especializada para la gestión de proyectos que permita, entre otros, la asignación de tareas y recursos, seguimiento a las actividades, avance del proyecto, ruta crítica, sobrecarga de recursos, entre otros.

	De la mejora al Procedimiento de Ingeniería de Software (GIC-PD-004) a futuro	
9	En la actividad AT2 de Clasificar solicitud, en el documento de apoyo GUÍA DE SOPORTE Y ASISTENCIA TÉCNICA (GIC-GU-009) no se indican las Reglas de Negocio por medio de las cuales se hace la clasificación en nuevos desarrollos (AT3), cambios (AT4) e incidencias (AT5) de los sistemas de información.	Para mayor facilidad en la ejecución de esta actividad es necesario indicar las reglas de negocio puntuales que se tienen y así no tener que estar revisando el documento de GUÍA DE SOPORTE Y ASISTENCIA TÉCNICA.
10	En la actividad AT2 de Clasificar solicitud, se sugiere luego de clasificar la solicitud continuar con los sub-procedimientos de nuevos desarrollos (AT3), cambios (AT4) e incidencias (AT5) de los sistemas de información, pero no se indica que hacer en caso de que la solicitud no corresponda con estos tres tipos de clasificación.	Es necesario incluir una actividad que indique que se debe hacer en caso que la solicitud no se enmarque en los tres tipos establecidos. Es recomendable revisar en todo el procedimiento si esta situación se repite, en tal sentido se deberá incluir la acción que se considere apropiada.
11	Para los sub-procedimientos de nuevos desarrollos (AT3), cambios (AT4) e incidencias (AT5) de los sistemas de información, en el Rol de Solicitante, no se observa una actividad de aprobación o VoBo en señal de conformidad de documentos generados en cada sub-procedimiento como: documento de arquitectura, análisis de historias de usuario y plan de trabajo.	En cada sub-procedimiento se debe incluir una actividad por parte del Solicitante relacionada con la revisión y aprobación de aquellos documentos que son base fundamental para llevar a cabo la atención del requerimiento realizado y para contar con el sustento de su decisión.
12	En los sub-procedimientos de Nuevo desarrollo de software actividad AT 10 Elaborar plan de pruebas y Cambios en los sistemas de información AT7 Actualizar plan de pruebas, las actividades son desarrolladas por el Analista, pero no se observa la participación bien sea del área de Aseguramiento de la Calidad o del Solicitante en la generación de dichos planes de prueba.	Es necesario considerar la participación activa del área de calidad o del solicitante del requerimiento en cuanto al diseño y ejecución de las pruebas que consideren que les puede asegurar que los desarrollos producen los resultados esperados.
13	Se observa que en el documento en general la columna de "Reglas de Negocio" no se utiliza.	Es necesario establecer el objetivo de este campo y si brinda algún lineamiento especial se debe diligenciar o en su defecto prescindir de colocarlo en el formato.