REFERENCIA	NOMBRE DE AUDITORIA	PROCESO AREA AUDITADA	FECHAS DE REALIZACIÓN (INICIO Y CIERRE)	FECHA DEL INFORME
A GTI 03	Tecnologías de la Información	Gestión del Sistema Único de Información Litigiosa del Estado	16 de Septiembre al 10 de octubre 2014	04/11/2014

AUDITOR RESPONSABLE
JORGE ANDRÉS MEDINA GALEANO
EQUIPO DE AUDITORES
N / A

1. CRITERIOS:

1.1 CALIDAD
No aplica
1.2 CONTROL INTERNO
• Normatividad legal y documentación interna aplicable al proceso, en particular asociada a políticas de gobierno en línea, seguridad de datos y control interno. • Controles generales de tecnología (administración de usuarios, gestión del cambio, respaldo a la información, infraestructura tecnológica y soporte usuario)

2. OBJETIVOS:

2.1CALIDAD
No Aplica
2.2 CONTROL INTERNO
Efectuar seguimiento a los desarrollos de tecnologías de la información y proyectos asociados al Sistema Único de Información Litigiosa.

3. ALCANCE:

Debido a que los esfuerzos de desarrollo se realizan sobre EKOGUI, se evaluó los requerimientos de EKOGUI y el soporte al aplicativo LITIGOB.

4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

La auditoría se desarrolló sin limitaciones mayores a organización de agendas, resaltando la oportuna atención de solicitudes y requerimientos.

5. DOCUMENTOS EXAMINADOS:

- Para la presente auditoría se aplicó muestreo sobre el total de los procedimientos de acuerdo a la periodicidad de los controles.
- Para los casos de análisis de usuarios, perfiles y casos de soporte se evaluó el universo de la muestra, debido a que la información se encuentra en medio digital. Se revisaron los controles a los diferentes dominios de tecnología en la siguiente información
- Información del sistema MANTIS de solicitudes de desarrollos de EKOGUI y soportes a LITIGOB
- Documentación de procedimientos e instructivos del sistema MANTIS
- Reporte de casos de MANTIS
- Reporte de usuarios y perfiles del sistema LITIGOB

- Decreto 1795 de 2007
- Decreto 2052 de 2014
- Consola de copias de seguridad
- Contrato UNE

6. RESUMEN DEL INFORME:

6.1 Elemento de la normas de calidad	Numeral de la Norma	Número de no conformidades
No aplica	No Aplica	No Aplica
Total de no conformidades	--	--

6.2 Normas de Control Interno (subsistema, componente, elemento)		
6.2 Normas de Control Interno (subsistema, componente, elemento)	**Criterio**	**Número de hallazgos**
Administración de usuarios	2	3
Plan de continuidad y contingencia	8	2
Total de hallazgos	--	5

7. INFORME

7.1 FORTALEZAS

- En el aplicativo MANTIS (software libre), se lleva a cabo la documentación y gestión de desarrollos y soportes, así como la creación de soportes, clasificación, aprobación, asignación (reasignación de ser necesario), documentación de la respuesta y cierre. * El aplicativo MANTIS cuenta con módulo de gestión de usuarios en donde se realiza la asignación de permisos, así como se evidenció documentación de sus procesos.
- Se concluye que la gestión de los soportes está controlada por el uso adecuado del sistema MANTIS y la oportunidad en la atención de las solicitudes.

7.2 CUMPLIMIENTO DE PRINCIPIOS

Se identificaron debilidades de control que pueden permitir la materialización de riesgos que afecten los criterios de la información tales como Integridad, Disponibilidad y Confiabilidad, citados dentro de la Política de Seguridad de la de la Agencia.

8. DESCRIPCIÓN DE LA (S) NO CONFORMIDAD (ES) Y/O HALLAZGO (S)

8.1. NO CONFORMIDADES EN SISTEMA DE CALIDAD

REQUISITO DE LA NORMA	NO CONFORMIDAD	OBSERVACIONES
No Aplica	No Aplica	No Aplica

8.2. HALLAZGOS EN SISTEMA DE CONTROL INTERNO

REQUISITO DE LA NORMA	HALLAZGOS	OBSERVACIONES
8. Continuidad y Contingencia	No existe un plan de contingencia del sistema, esto es que, si el proveedor falla en el servicio la operación del sistema litigioso se detendría exponiendo a la Entidad a una pérdida de	

	disponibilidad de la información y perdida de la buena imagen de la Entidad.	
2. Administración de usuarios	Luego de revisar los usuarios activos del sistema se validó la aplicación de la recomendación dada a los administradores de entidad de ingresar el número de cédula en el campo Identificación y así mismo utilizarlo como Usuario, encontrando que los campos no validan que sólo se ingresen números y no símbolos o caracteres especiales. • Se encontró que 92 usuarios utilizan diferentes nombres de Usuario usando caracteres especiales, textos o números que no se relacionan al documento de identidad • Se identificaron 14 diferentes usuarios con el mismo texto como Usuario "APODERADO". • El sistema no pide contraseñas seguras ni el cambio de la inicial dada por el administrador la cual por definición es 123 Por lo anterior no se garantiza el principio de confidencialidad e integridad de la información. Según el reporte de usuarios del sistema, se identificaron 36 usuarios que fueron creados con la misma información en todos los campos para la misma entidad y con los mismos permisos en más de dos ocasiones, como el caso de la apodera de la Registraduría Nacional del Estado Civil, usuaria Dora Maria Gomez, que tiene 8 registros similares según reporte del sistema"	
8. Continuidad y Contingencia	El sistema que es soportado bajo infraestructura del proveedor UNE en un centro de alta disponibilidad, sin embargo no se cuenta con un documento o plan de contingencia	
2. Administración de usuarios	• Se identificaron 24 perfiles creados de los cuales tres de ellos no se observa que tengan permisos asignados. • Solo 14 perfiles están asignados a los usuarios activos del sistema. • Se identificaron 426 usuarios activos en los que el reporte no informa que tipo de perfil tiene asignado. • Se encontró dos entidades definidas como entidades de prueba con 81 usuarios activos en el sistema."	
2. Administración de usuarios		No se realiza una revisión como control a los perfiles existentes, por el contrario se identificaron perfiles no asignados, perfiles sin permisos o perfiles con un único usuario.

2. Administración de usuarios		Luego de la revisión del reporte del sistema se identificaron 24 perfiles creados de los cuales, de tres de ellos no se observa que tengan permisos asignados, así como solo 14 perfiles están asignados a los usuarios activos del sistema. En la entrevista se determinó que no se realiza una revisión periódica (por lo menos anual) a los perfiles y permisos del sistema.
2. Administración de usuarios		Se identificaron 426 usuarios activos en los que el reporte no informa que tipo de perfil tiene asignado.
3. Políticas y manuales		Si bien en el Decreto 1795 de 2007 estableció funciones y responsabilidades de manera general frente al sistema litigioso, con el actual Decreto 2052 de 2014, se precisan claras funciones y responsabilidades de los usuarios y actores del sistema de defensa del Estado. De otra parte se resalta que el citado Decreto 2052, le asigna un carácter vinculante a los manuales de usuario y otros documentos que la Entidad expida.
5. Copias de seguridad		Las copias que se almacenan externamente son almacenadas en un disco duro que son transportadas mensualmente por funcionarios de la Agencia sin un procedimiento definido, sin estándares de transporte ni de almacenamiento, exponiendo a la Agencia a pérdida o fugas de la información y perdida de la disponibilidad de la misma.
8. Continuidad y Contingencia		No se realizan pruebas al plan de contingencia debido a que no se cuenta con el escenario contingente para el sistema de la Entidad
8. Continuidad y Contingencia		No se han documentado y actualizado los procesos y pruebas de continuidad por ausencia del escenario contingente.
8. Continuidad y Contingencia		No se han realizado los documentos de análisis de impacto en el negocio, BIA, por tal razón no se cumple con estudios previos de los planes de continuidad

9. RECOMENDACIONES:

Controles en la gestión del cambio y soporte al usuario.

- Continuar documentando mediante herramientas como MANTIS los desarrollos y soportes;
- Implementar un comité de control de cambios con participación de un agente evaluador de riesgos.

Controles políticas del sistema

- La Agencia tiene una gran oportunidad para reglamentar todos los aspectos relacionados con la administración del sistema de manera tal que se pueda hacer un eficiente control hacia las entidades y garantizar los criterios de la información.

- Se debe tener en cuenta que el Decreto 2052 de 2014 está orientado al sistema EKOGUI motivo por el cual se debe analizar su aplicación sobre el sistema LITIGOB que sigue vigente al momento.

Controles de gestión de usuarios.

- Establecer controles tendientes a garantizar el acceso exclusivo a los usuarios que requieran acceso a la información y al sistema;
- Restringir en los campos de identificación y usuario a solo caracteres numéricos;
- Establecer políticas de contraseñas de autenticación fuertes;
- Incluir en los controles del sistema de autenticación EKOGUI, la validación de los campos para evitar duplicidad de registros;
- Establecer como actividad de control la realización de una revisión periódica a los perfiles y permisos del sistema, así como a las entidades creadas en el sistema.

Controles de copias de respaldo

Con el proceso de adquisición del sistema para Backups que adelanta la Agencia, se recomienda establecer un procedimiento para la toma de copias de seguridad que garanticen la supervisión diaria, las pruebas a las copias y un correcto transporte y almacenamiento de las copias.

Controles del plan de contingencia

Establecer un plan de contingencia y continuidad del servicio y de la operación en atención a estudios de evaluación del riesgo de impacto en el negocio.

Firma Auditor Designado y Equipo Auditor	Firma Jefe de Control Interno ANDJE

Versión	Fecha Aprobación	Naturaleza del Cambio
0	08-05-2013	Documento Original.